Dreiundvierzigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2014

gemäß § 30 des Hessischen Datenschutzgesetzes

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

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

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

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 43. Tätigkeitsbericht

Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AGB	Allgemeine Geschäftsbedingungen
AnwBl	Anwaltsblatt
App	application (Anwendungssoftware für mobile Betriebssysteme)
Artikel 10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet
AufenthV	Aufenthaltsverordnung
AuR	Zeitschrift „Arbeit und Recht“
BCC	Blind Carbon Copy
BCRs	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BeckRS	Beck-Rechtsprechung
Berliner KhsVO	Berliner Krankenhaus-Verordnung
BetrVG	Betriebsverfassungsgesetz
BfV	Bundesamt für Verfassungsschutz
BfV-Gesetz	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHZ	Entscheidungssammlung des Bundesgerichtshof in Zivilsachen
BIC	International gültige Bankleitzahl (Bank Identifier Code)
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern
BRAK-Mitt.	Mitteilungen der Bundesrechtsanwaltskammer
BRAO	Bundesrechtsanwaltsordnung

BRDrucks.	Bundesratsdrucksache
BRJ	Bonner Rechtsjournal
BSI	Bundesamt für Sicherheit in der Informationstechnik
BTDrucks.	Bundestagsdrucksache
BTLE-Subgroup	Unterarbeitsgruppe „Borders, Travel, Law Enforcement“
BtMG	Betäubungsmittelgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands e. V.
BVerfG	Bundesverfassungsgericht
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BVerwGE	Entscheidungssammlung des Bundesverwaltungsgerichts
BvR	Registerzeichen bzw. Aktenzeichen des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
CC	Carbon Copy
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
d. h.	das heißt
DAPIX	Working Party on Information Exchange and Data Protection
DaTraGebV	Datentransparenz-Gebührenverordnung
DB	Zeitschrift „Der Betrieb“
DÖV	Zeitschrift „Die öffentliche Verwaltung“
DRV Bund	Deutsche Rentenversicherung Bund
DSGVO	Datenschutz-Grundverordnung
DuD	Zeitschrift „Datenverarbeitung und Datenschutz“
e. V.	eingetragener Verein
EES	Einreise- und Ausreisesystem (Entry-Exit-System)
eID	elektronische Identifizierung
EStG	Einkommensteuergesetz

etc.	et cetera
EU	Europäische Union
EU-LISA	European Agency for the Operational Management of large-scale IT-Systems in the area of freedom, security and justice
EURODAC	European Dactyloscopy
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
evtl.	eventuell
EWR	Europäischer Wirtschaftsraum
FBAG	Gesetz über die Erhebung der Fehlbelegungsabgabe in der sozialen Wohnraumförderung
FD-ArbR	Zeitschrift „Fachdienst Arbeitsrecht“
FinA	Finanzarchiv
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GPEN	Global Privacy Enforcement Network
GrCh	Charta der Grundrechte der Europäischen Union
GRUR	Zeitschrift „Gewerblicher Rechtsschutz und Urheberrecht“
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
HDSG	Hessisches Datenschutzgesetz
HGO	Hessische Gemeindeordnung
HJagdG	Hessisches Jagdgesetz
HKM	Hessisches Kultusministerium
HMG	Hessisches Meldegesetz
HPVG	Hessisches Personalvertretungsgesetz
HRDG	Hessisches Rettungsdienstgesetz
HSchulG	Hessisches Schulgesetz
HSM	Hessisches Ministerium für Soziales und Integration
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HSÜG	Hessisches Sicherheitsüberprüfungsgesetz
https	Hypertext Transfer Protocol Secure
HVerfSchG	Hessisches Gesetz über das Landesamt für Verfassungsschutz

HVGG	Hessisches Gesetz über das öffentliche Vermessungs- und Geoinformationswesen
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HWaldG	Hessisches Waldgesetz
HZD	Hessische Zentrale für Datenverarbeitung
IaaS	Infrastructure as a Service
IBAN	Internationale Kontonummer (International Bank Account Number)
InfAuslR	Zeitschrift „Informationsbrief Ausländerrecht“
IP	Internetprotokoll
IT	Informationstechnik
JuS	Zeitschrift „Juristische Schulung“
K&R	Zeitschrift „Kommunikation und Recht“
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
KKR	Klinische Krebsregister
KWG	Kreditwesengesetz
LÄK Hessen	Landesärztekammer Hessen
LfV	Landesamt für Verfassungsschutz
LKHG M-V	Krankenhausgesetz für das Land Mecklenburg-Vorpommern
LUSD	Lehrer- und Schüler-Datenbank
m. E.	meines Erachtens
MAC	media access control (Mediumzugriffssteuerung)
MDR	Monatszeitschrift für Deutsches Recht
MIR	Onlinepublikation „Medien Internet und Recht“
MMR	Zeitschrift „MultiMedia und Recht“
MRRG	Melderechtsrahmengesetz
NADIS-WN	Nachrichtendienstliches Informationssystem und Wissensnetz
NJ	Zeitschrift „Neue Justiz“
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NStZ-RR	Neue Zeitschrift für Strafrecht – Rechtsprechungsreport

NZA	Neue Zeitschrift für Arbeitsrecht
NZA-RR	Neue Zeitschrift Arbeitsrecht – Rechtsprechungsreport
NZF	Nassauischer Zentralstudienfonds
NZFam	Neue Zeitschrift für Familienrecht
OH KIS	Orientierungshilfe für Krankenhausinformationssysteme
openJur	eine freie juristische Fachdatenbank
OWiG	Gesetz über Ordnungswidrigkeiten
PaaS	Platform as a Service
PAuswG	Personalausweisgesetz
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PIA	Privacy impact assessment
PStG	Personenstandsgesetz
PVS	Praxisverwaltungssystem
Rdnr.	Randnummer
RdV	Zeitschrift „Recht der Datenverarbeitung“
RFID	radio-frequency identification
RiW	Zeitschrift „Recht der Internationalen Wirtschaft“
RöV	Röntgenverordnung
RP Kassel	Regierungspräsidium Kassel
RTP	Registrierungsprogramm für Vielreisende (Registered Traveller Program)
s.	siehe
S.	Seite
SaaS	Software as a Service
SG	Soldatengesetz
SGB	Sozialgesetzbuch
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Entity
SIS II	Schengener Informationssystem II
sog.	sogenannte/er/es
SSL	Secure Sockets Layer
StB	Zeitschrift „Der Steuerberater“

StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StV	Zeitschrift „Strafverteidiger“
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
TMG	Telemediengesetz
u. a.	unter anderem/und andere
VIS	Visa-Informationssystem
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
wistra	Zeitschrift für Wirtschafts- und Steuerstrafrecht
WLAN	wireless local area network (drahtloses, lokales Netzwerk)
WpDVerOV	Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung
WPflG	Wehrpflichtgesetz
WpHG	Wertpapierhandelsgesetz
WRP	Zeitschrift „Wettbewerb in Recht und Praxis“
z. B.	zum Beispiel
ZA	Zeitschrift für Jurastudium und Ausbildung
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht
ZPO	Zivilprozessordnung
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	Zeitschrift für Urheber- und Medienrecht Rechtsprechungsdienst

Register der Rechtsvorschriften

AEUV	Vertrag über die Arbeitsweise der Europäischen Union i. d. F. vom 09.05.2008 (ABl. EG C 115 S. 47), zuletzt geändert durch die Akte vom 09.12.2011 (ABl. EU L 112 S. 21)
Artikel 10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 26.06.2001 (BGBl. I S. 1254, 2298), zuletzt geändert durch Gesetz vom 12.06.2015 (BGBl. I S. 926)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) i. d. F. vom 25.02.2008 (BGBl. I S. 162), zuletzt geändert durch Gesetz vom 23.12.2014 (BGBl. I S. 2439)
AufenthV	Aufenthaltsverordnung i. d. F. vom 25.11.2004 (BGBl. I S. 2945), zuletzt geändert durch die Verordnung vom 08.04.2015 (BGBl. I S. 599)
BDSG	Bundesdatenschutzgesetz i. d. F. vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 25.02.2015 (BGBl. I S. 162)
Berliner KhsVO	Verordnung über Errichtung und Betrieb von Krankenhäusern, Krankenhausaufnahme, Führung von Krankengeschichten und Pflegedokumentationen und Katastrophenschutz in Krankenhäusern (Berliner Krankenhaus-Verordnung) vom 30.08.2006 (GVBl. für Berlin S. 907)
Berufsordnung der Landesapothekerkammer Hessen	Berufsordnung der Landesapothekerkammer Hessen, beschlossen von der Delegiertenversammlung der Landesapothekerkammer Hessen am 14.03.2012, genehmigt durch Erlass des Hessischen Sozialministeriums am 29.03.2012 (PZ Nr. 18/2012, S. 1624 und DAZ Nr. 18/2012, S. 2301)
BetrVG	Betriebsverfassungsgesetz i. d. F. vom 25.09.2001 (BGBl. I S. 2518), zuletzt geändert durch Gesetz vom 20.04.2013 (BGBl. I S. 868)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42, 2909, 2003 S. 738), zuletzt geändert durch Gesetz vom 21.04.2015 (BGBl. I S. 610)
BMG	Bundesmeldegesetz i. d. F. vom 03.05.2013 (BGBl. I S. 1084), zuletzt geändert durch Gesetz vom 20.11. 2014 (BGBl. I S. 1738)
BRAO	Bundesrechtsanwaltsordnung i. d. F. vom 01.08.1959 (BGBl. I S. 565), zuletzt geändert durch Gesetz vom 10.10.2013 (BGBl. I S. 3786)

BtMG	Gesetz über den Verkehr mit Betäubungsmitteln (Betäubungsmittelgesetz) i. d. F. vom 01.03.1994 (BGBl. I S. 358), zuletzt geändert durch Gesetz vom 20.05.2015 (BGBl. I S. 725)
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz i. d. F. vom 20.12.1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Gesetz vom 20.06.2013 (BGBl. I S. 1602)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) i. d. F. vom 21.09.1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 21.01.2015 (BGBl. I S. 10)
DaTraGebV	Verordnung zur Erhebung von Gebühren und Auslagen für die Bereitstellung von Daten nach den Regelungen der Datentransparenzverordnung (Datentransparenz-Gebührenverordnung) i. d. F. vom 30.04.2014 (BGBl. I S. 458)
DSGVO	Datenschutz-Grundverordnung i. d. F. des Vorschlags der Europäischen Kommission vom 25.01.2012 (KOM(2012) 11 endgültig; 2012/001 (COD) und des Beschlusses des Europäischen Parlaments vom 12.03.2014 i. R. der 1. Lesung zu dem o. g. Vorschlag der Europäischen Kommission (Interinstitutionelles Dossier des Rats der Europäischen Union vom 27.03.2014, 2012/001 (COD); 7427/1/14, REV 1)
EStG	Einkommensteuergesetz i. d. F. vom 08.10.2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Gesetz vom 01.04.2015 (BGBl. I S. 434)
GewO	Gewerbeordnung i. d. F. vom 22.02.1999 (BGBl. I S. 202), zuletzt geändert durch Gesetz vom 15.04.2015 (BGBl. I S. 583)
GG	Grundgesetz für die Bundesrepublik Deutschland (BGBl. III, Gliederungsnummer 100-1), zuletzt geändert durch Gesetz vom 23.12.2014 (BGBl. I S. 2438)
GRCh	Charta der Grundrechte der Europäischen Union i. d. F. vom 18.12.2000 (ABl. EG 2000/C 364/01 S. 1 und 2012/C 326/02 S. 391) sowie die Erläuterungen zur Charta der Grundrechte vom 14.12.2007 (ABl. EG 2007/C 303/02 S. 17)
GVG	Gerichtsverfassungsgesetz i. d. F. vom 09.05.1975 (BGBl. I S. 1077), zuletzt geändert durch Gesetz vom 21.01.2015 (BGBl. I S. 10)

GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) i. d. F. vom 13.08. 2008 (BGBl. I S. 1690), zuletzt geändert durch Gesetz von 12.06.2015 (BGBl. I S. 926)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 07.01.1999 (GVBl. I S. 98), zuletzt geändert durch Gesetz vom 20.05.2011 (GVBl. I S. 208)
HGO	Hessische Gemeindeordnung i. d. F. vom 07.03.2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 28.03.2015 (GVBl. I S. 1582), berichtigt am 22.04.2015 (GVBl. S. 188)
HJagdG	Hessisches Jagdgesetz i. d. F. vom 05.06.2001 (GVBl. I S. 271), zuletzt geändert durch Gesetz vom 27.06.2013 (GVBl. S. 458)
HMG	Hessisches Meldegesetz i. d. F. vom 10.03.2006 (GVBl. I S. 66), zuletzt geändert durch Gesetz vom 22.11.2010 (GVBl. I S. 403, 404)
HPVG	Hessisches Personalvertretungsgesetz i. d. F. vom 24.03.1988 (GVBl. I 1988, 103), zuletzt geändert durch Gesetz vom 24.03.2015 (GVBl. I S. 118)
HRDG	Hessisches Rettungsdienstgesetz i. d. F. vom 16.12. 2010 (GVBl. I S. 646), zuletzt geändert durch Gesetz vom 13.12.2012 (GVBl. S. 622)
HSchulG	Hessisches Schulgesetz i. d. F. vom 14.12.2009 (GVBl. S. 666), zuletzt geändert durch Gesetz vom 28.09.2014 (GVBl. S. 218)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14.01.2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 29.04.2015 (GVBl. S. 202)
HSÜG	Hessisches Sicherheitsüberprüfungsgesetz i. d. F. vom 19.12.2014 (GVBl. S. 364)
HVerfSchG	Hessisches Gesetz über das Landesamt für Verfassungsschutz i. d. F. vom 19.12.1990 (GVBl. I S. 753), zuletzt geändert durch Gesetz vom 27.06.2013 (GVBl. S. 444)
HVGG	Hessisches Gesetz über das öffentliche Vermessungs- und Geoinformationswesen i. d. F. vom 06.09.2007 (GVBl. I S. 548), zuletzt geändert durch Gesetz vom 27.09.2012 (GVBl. I S. 290)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15.01.2010 (GVBl. I S. 18), zuletzt geändert durch Gesetz vom 13.12.2012 (GVBl. S. 622)
HWaldG	Hessisches Waldgesetz i. d. F. vom 27.06.2013 (GVBl. S. 458), zuletzt geändert durch Gesetz vom 16.07.2014 (GVBl. S. 186)

Informationssicherheitsleitlinie für die Hessische Landesverwaltung, 2010	StAnz 2010 S. 106
IT-Sicherheitsleitlinie für die Hessische Landesverwaltung, 2004	StAnz 2004 S. 3827
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz) i. d. F. vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Gesetz vom 12.06.2015 (BGBl. I S. 926)
LKHG M-V	Krankenhausgesetz für das Land Mecklenburg-Vorpommern vom 20.05.2011 (GVOBl. M-V, S. 327)
MRRG	Melderechtsrahmengesetz i. d. F. vom 19.04.2002 (BGBl. I S. 1342), zuletzt geändert durch Gesetz vom 28.08.2013 (BGBl. I S. 3458)
OH KIS	Orientierungshilfe für Krankenhausinformationssysteme, erstellt von den Arbeitskreisen „Gesundheit und Soziales“ und „Technik“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche, 2. Fassung, Stand März 2014
OWiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19.02. 1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 13.05.2015 (BGBl. I S. 706)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) i. d. F. vom 18.06. 2009 (BGBl. I S. 1346), zuletzt geändert durch Gesetz vom 07.08.2013 (BGBl. I S. 3154)
PStG	Personenstandsgesetz vom 19.02.2007 (BGBl. I S. 122), zuletzt geändert durch Gesetz vom 28.08.2013 (BGBl. I S. 3458)
Richtlinie 1999/93/EG	Richtlinie des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 1999/L 013 S. 12)
Richtlinie 95/46/EG	Richtlinie des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG 1995/L 281 S. 31)
Richtlinie 98/79/EG	Richtlinie des Europäischen Parlaments und des Rates vom 27.10.1998 über In-vitro-Diagnostika (ABl. EG 1998/L 331 S. 1)
Richtlinie 2005/60EG	Richtlinie des Europäischen Parlaments und des Rates vom 26.10.2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (ABl. EG 2005/L 309 S. 15)

Richtlinie 2006/24/EG	Richtlinie des Europäischen Parlaments und des Rates vom 15.03.2006 zur Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden (ABl. EG 2006/L 105 S. 54)
RöV	Verordnung über den Schutz vor Schäden durch Röntgenstrahlen (Röntgenverordnung) i. d. F. vom 30.04. 2003 (BGBl. I S. 604), zuletzt geändert durch Verordnung vom 11.12.2014 (BGBl. I S. 2010)
SG	Gesetz über die Rechtsstellung der Soldaten (Soldatengesetz) i. d. F. vom 30.05.2005 (BGBl. I S. 1482), zuletzt geändert durch Gesetz vom 13.05.2015 (BGBl. I S. 706)
SGB II	Sozialgesetzbuch Zweites Buch – Grundsicherung für Arbeitsuchende i. d. F. vom 24.12.2003 (BGBl. I S. 2954), zuletzt geändert durch Gesetz vom 24.06.2015 (BGBl. I S. 974)
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung – i. d. F. vom 20.12.1988, BGBl. I S. 2477), zuletzt geändert durch Gesetz vom 15.04.2015 (BGBl. I S. 583)
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – i. d. F. vom 11.09.2012 (BGBl. I S. 2022), zuletzt geändert durch Gesetz vom 21.01.2015 (BGBl. I S. 10)
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz i. d. F. vom 18.01.2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 11.08.2014 (BGBl. I S. 1348)
StGB	Strafgesetzbuch i. d. F. vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 12.06.2015 (BGBl. I S. 926)
StPO	Strafprozessordnung i. d. F. vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 12.06.2015 (BGBl. I S. 926)
TKG	Telekommunikationsgesetz i. d. F. vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 25.07.2014 (BGBl. I S. 1266)
TMG	Telemediengesetz i. d. F. vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Art. 2 des Gesetzes vom 01.04.2015 (BGBl. I S. 434)
Verordnung über die Verarbeitung personenbezogener Daten und statistische Erhebungen an Schulen	vom 04.02.2009 (ABl. des Hessischen Kultusministeriums Nr. 3/2009 S. 131)
VwVfG	Verwaltungsverfahrensgesetz i. d. F. vom 23.01.2003 (BGBl. I S. 102), zuletzt geändert durch Gesetz vom 25.07.2013 (BGBl. I S. 2749)

WpDVerOV	Verordnung zur Konkretisierung der Verhaltensregeln und Organisationsanforderungen für Wertpapierdienstleistungsunternehmen (Wertpapierdienstleistungs-Verhaltens- und Organisationsverordnung) i. d. F. vom 20.07.2007 (BGBl. I S. 1432), zuletzt geändert durch die Verordnung vom 15.07.2014 (BGBl. I S. 956)
WPflG	Wehrpflichtgesetz i. d. F. vom 15.08.2011 (BGBl. I S. 1730), zuletzt geändert durch Gesetz vom 03.05. 2013 (BGBl. I S. 1084)
WpHG	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz) i. d. F. vom 09.09.1998 (BGBl. I S. 2708), zuletzt geändert durch Gesetz vom 01.04.2015 (BGBl. I S. 434)
ZPO	Zivilprozessordnung i. d. F. vom 05.12.2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Gesetz vom 08.07.2014 (BGBl. I S. 890)
Zwei-plus-Vier-Vertrag	Vertrag über die abschließende Regelung in Bezug auf Deutschland (Regelungsvertrag) i. d. F. vom 12.09.1990 (BGBl. II S. 1317)

Kernpunkte

1. Zahlreiche Anfragen und Beschwerden betrafen das Scoring der Schufa. Meine Überprüfungen ergaben keinen Anlass zur Kritik. Hinsichtlich des Inhalts der Datenübersicht für Betroffene und des Verfahrens zum Erhalt einer Datenübersicht hat die Schufa aufgrund meiner Kritik Änderungen vorgenommen.

2. „Damit Sie den Überblick behalten", „Zu Ihrer eigenen Sicherheit wird dieses Gebäude videoüberwacht" – „Mittels Wildkamera stets im Blick, wann das Schwarzwild zur Kirrung kommt" – vermeintliche (gute?) Gründe zur Installation von Videoüberwachungskameras gibt es viele. Leider verlieren die Hersteller der Produkte, Händler und nicht zuletzt die Kamerabetreiber bei Vertrieb und Installation der Anlagen allzu oft die gesetzlichen Bestimmungen aus den Augen.

3. Der punktuelle Einsatz von sog. „BodyCams" im Rahmen von Personenkontrollen ist grundsätzlich möglich. Gegen eine Ausweitung auch auf Tonaufnahmen in diesem Kontext bestehen erhebliche Bedenken.

4. Die namentliche Nennung von privaten Kunden als Referenzen auf der Webseite eines Unternehmens ist nur mit einer ausdrücklichen Einwilligung der betroffenen Kunden zulässig. Wurden keine Einwilligungen eingeholt, können zwar erfolgreiche Projekte des Unternehmens zu Werbezwecken veröffentlicht werden, jedoch nur, wenn die Angaben anonym und die privaten Kunden bzw. Auftraggeber nicht identifizierbar sind.

5. Bürgerbüros müssen so eingerichtet werden, dass Bürgerinnen und Bürger die Möglichkeit haben, ihre Anliegen einem Mitarbeiter der Verwaltung vorzutragen, ohne dass Dritte mithören können.

6. Daten, die aufgrund einer Rechtsgrundlage entweder öffentlich bekannt gemacht oder öffentlich ausgelegt werden und damit jedem interessierten Bürger zur Einsichtnahme zugänglich sind, dürfen ohne ausdrückliche Rechtsgrundlage nicht automatisch auch im Internet veröffentlicht werden.

7. Dem Europäischen Gerichtshof zufolge kann eine Person, wenn bei einer anhand ihres Namens durchgeführten Suche in der Trefferliste der Suchmaschine ein Link zu einer Webseite mit Informationen über sie angezeigt wird, unter bestimmten Voraussetzungen vom Suchmaschinenbetreiber verlangen, den Link aus der Trefferliste zu entfernen. Das Urteil stellt die Aufsichtsbehörden vor eine Reihe von Auslegungsfragen.

8. Arztpraxen müssen sicherstellen, dass unbefugte Dritte insbesondere im Empfangsbereich keinen Einblick in Patientenakten nehmen können.
9. Bei der Schließung von Krankenhäusern, insbesondere in Fällen von Insolvenz, gibt es ein hohes Risiko, dass die Patientenakten nicht sicher verwahrt werden und die Verwahrung bzw. Vernichtung nicht mehr sichergestellt wird. Vor dem Hintergrund aktueller Fälle in Hessen habe ich das Hessische Ministerium für Soziales und Integration kontaktiert. Gemeinsam mit der Landesärztekammer Hessen, der Hessischen Krankenhausgesellschaft, dem Berufsverband der in Deutschland tätigen Insolvenzverwalter und weiteren Stellen sollen praktikable Regelungen und Problemlösungen entwickelt werden.
10. Im Jahr 2014 wurde die Orientierungshilfe für Krankenhausinformationssysteme von den Datenschutzbeauftragten aktualisiert. Meine Prüfungen vor Ort habe ich fortgesetzt. Probleme habe ich insbesondere festgestellt hinsichtlich der verbindlichen Festlegung der Abläufe bei der Protokollierung und deren Umsetzung.
11. Beim Einsatz von Wasserzählern, die per Funk ausgelesen werden, müssen nicht nur die rechtlichen Rahmenbedingungen geschaffen werden. Die eingesetzte Technik muss auch bestimmte Anforderungen erfüllen.

1. Einführung

1.1
Allgemeines

1.1.1
Öffentliche Wahrnehmung des Datenschutzes

Der Datenschutz hatte auch 2014 Konjunktur. Die nachrichtendienstlichen Tätigkeiten insbesondere der USA, europäische Vollharmonisierungsambitionen und spektakuläre Gerichtsentscheidungen führten dazu, dass der Datenschutz sich nach wie vor großer Medienaufmerksamkeit erfreute. Bedauerlicherweise hinderte das einen Gutteil der Bevölkerung nicht an einem recht sorglosen Umgang mit den eigenen Daten, insbesondere bei der Nutzung sozialer Netzwerke.

1.1.2
National Security Agency

Der sog. NSA-Datenschutzskandal hat eine Flut von Veröffentlichungen nach sich gezogen (Brands, NSA, BND & Co.: Die Möglichkeiten der Geheimdienste: Technik, Auswertung, Gegenmaßnahmen, 2014; Greenwald, Die globale Überwachung – der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, 2014; Harding, The Snowden Files. The Inside Story of the World's Most Wanted Man, London 2014, deutsch: Edward Snowden: Geschichte einer Weltaffäre, 2014; Rosenbach/Stark, Der NSA-Komplex. Edward Snowden und der Weg in die totale Überwachung, 2014). Zumeist werden dabei politische Folgerungen auf Spekulationen im Tatsächlichen gestützt. Dadurch wächst die Gefahr, dass subjektive Ressentiments und das eigene politische Vorverständnis zum Maßstab gemacht und die Rechtslage verkannt wird. Das bedeutet aber nicht, dass zu den unbestrittenen Eingriffen jedenfalls in die deutsche Territorialhoheit und damit „volle" Souveränität (Art. 7 Abs. 2 Vertrag über die abschließende Regelung in Bezug auf Deutschland) sowie in Persönlichkeitsrechte deutscher Staatsangehöriger gar keine rechtliche Stellungnahme abgegeben werden dürfte. Ich sah mich daher gehalten, in meiner Rede im Plenum des Hessischen Landtags zum 41. Tätigkeitsbericht am 21. Mai 2014 Folgendes zu erklären:

„Ich habe mich mit Äußerungen zur NSA-Affäre weitgehend zurückgehalten, weil es sich vorwiegend um eine politische Angelegenheit handelt, für die ich nicht zuständig bin. Was mich aber erstaunt, ist, dass die rechtliche Dimension der Affäre praktisch überhaupt nicht thematisiert wird. Spionage

ist völkerrechtlich erlaubt. Das macht aber Spione nicht zu Kombattanten und rechtfertigt nicht deren Verstöße gegen die jeweils nationale Rechtsordnung. Es ist somit weniger bedeutsam, dass uns fremde Geheimdienste ausspioniert haben und ausspionieren, auch wenn die nahezu vollständige Erfassung der deutschen Bevölkerung einen unfreundlichen, geradezu beleidigenden Akt darstellt. Entscheidend ist, wozu die erhobenen Daten verwendet werden. Die Weitergabe von Betriebs- und Geschäftsgeheimnissen wäre beispielsweise ein Rechtsbruch, der mit Mitteln des internationalen Rechts geahndet werden könnte. Über die Abhörfolgen ist somit eine rechtliche Diskussion zu führen, bei der datenschutzrechtliche Gesichtspunkte mit zu berücksichtigen sind."

Die rechtliche Bewertung kam mittlerweile in Gang (vgl. nur Deiseroth, Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, ZRP 2013, 194; Petri, Déjà vu – datenschutzrechtliche Aufarbeitung der PRISM-Affäre, ZD 2013, 557; Ewer/Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30; Roßnagel/Jandt/Richter, Die Zulässigkeit der Übertragung personenbezogener Daten in die USA im Kontext der NSA-Überwachung, DuD 2014, 545; Talmon, Das Abhören der Kanzlerhandys und das Völkerrecht, BRJ (Bonner Rechtsjournal) 01/2014, S. 6 ff. Kipker/Voskamp, PRISM und staatliche Schutzpflichten – ein politisches Märchen?, RDV 2014, 84). Die zentralen Fragen des konkreten Umgangs mit Nachrichtendiensten werden aber selten gestellt. Beliebter sind allgemein gehaltene Forderungen nach einer stärkeren Kontrolle der Nachrichtendienste etwa durch die Ausweitung des Richtervorbehalts. Ob dies zur Gewährleistung des Grundrechts auf informationelle Selbstbestimmung zielführend wäre, erscheint fraglich (vgl. hierzu Weisser, Der Richtervorbehalt im Nachrichtendienstrecht, DÖV 2014, 831). Erfolgversprechender dürften einzelne Maßnahmen sein, die darauf abzielen, die parlamentarische Kontrolle der Geheimdienste zu intensivieren. Auch der Hessische Datenschutzbeauftragte wird seinen Kontrollfunktionen in diesem Zusammenhang verschärft nachkommen.

1.1.3
Europäische Datenschutz-Grundverordnung

1.1.3.1
Entwicklung

Im Berichtszeitraum trat die Harmonisierung des europäischen Datenschutzrechts in die entscheidende Phase (siehe hierzu unten Ziff. 1.2 vgl.

Koós, Das Vorhaben eines einheitlichen Datenschutzes in Europa – Aktueller Stand des europäischen Gesetzgebungsverfahrens, ZD 2014, 9; Roßnagel/Kroschwald: Was wird aus der Datenschutz-Grundverordnung? – Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument, ZD 2014, 495). Nachdem der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) des Europäischen Parlaments am 21. Oktober 2013 die durch den Europaabgeordneten Jan Philipp Albrecht ausgearbeitete Verhandlungsposition zur Datenschutz-Grundverordnung mit 49 Ja-Stimmen, einer Gegenstimme und drei Enthaltungen angenommen hatte, stimmte das Plenum des Europäischen Parlaments am 12. März 2014 über die EU-Datenschutzreform ab. Von 653 Abgeordneten stimmten 621 für den vorgeschlagenen Text, zehn Abgeordnete stimmten dagegen und 22 Abgeordnete enthielten sich. Die Legislative (Entschließung des Europäischen Parlaments (COM[2012]0011 – C7-0025/2012 – 2012/0011[COD]) korrigierte zwar etliche Unklarheiten, praxisferne Vorschläge und Unstimmigkeiten aus der Kommissions-Fassung (so BvD-News 1/2014, S. 12), war aber erst durch die von der griechischen Präsidentschaft vorgenommene Beschränkung auf Kapitel V (Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen; Ratsdokument 10349/14 vom 22. Mai 2013) verhandlungstauglich. Auf der Tagung vom 26./27. Juni 2014 einigten sich die Staats- und Regierungschefs auf folgende Schlussfolgerung des Europäischen Rats (EUCO 79/14 Ziff. I 4):

„Bei der weiteren Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts in den nächsten Jahren wird es entscheidend sein, den Schutz und die Förderung der Grundrechte, einschließlich des Datenschutzes, zu gewährleisten und gleichzeitig auf die Sicherheitsbelange, auch in den Beziehungen zu Drittländern, einzugehen sowie bis 2015 einen soliden allgemeinen Rahmen für den Datenschutz in der EU zu verabschieden."

Das Parlament erwartete daraufhin eine Einigung im Rat, damit die Verhandlungen zwischen Europäischem Parlament, Rat und Europäischer Kommission („Trilog") beginnen konnten. Auf der Grundlage der legislativen Entschließung des Parlaments schien jedoch eine Einigung kaum zu erzielen zu sein, da die meisten der im 41. Tätigkeitsbericht unter Ziff. 1.2 näher ausgeführten Kritikpunkte fortbestanden (vgl. noch Ronellenfitsch, Fortentwicklung des Datenschutzrechts, ZD 2012, 561; Herrmann: Anmerkung zur Reform des europäischen Datenschutzrechts – Harmonisierung unter Wahrung hoher datenschutzrechtlicher Standards, ZD 2014, 439). Die Verhandlungen dauerten indessen im Rat fort (Nguyen, Die Verhandlungen um die EU-Datenschutz-Grundverordnung unter litauischer Ratspräsidentschaft, RDV 2014, 26).

1.1.3.2
Kritik

Den deutschen Verhandlungsteilnehmern im EU-Ministerrat wurde vorgeworfen, sie zählten zu den „Bremsern“ des EU-Datenschutzes (Selmayr, Nach PRISM: Endet jetzt die Ambivalenz der deutsche Position zum EU-Datenschutz?, ZD 2013, 525; Schaar, EU-Datenschutz: Schluss mit der Verzögerungstaktik, ZD 2014, 113). Die gerügten Kompetenzüberschreitungen bestünden schon bei der Datenschutz-RL, was bislang niemand beanstandet habe. Der Vorwurf ist zurückzuweisen. Auch unter Berücksichtigung des acquis communautaire erstarkt durch rügefreie Beanspruchung eine angemaßte nicht zur wahren Kompetenz. Der Vorwurf geht auch sonst fehl. Die Amtspflicht der deutschen Verhandlungsteilnehmer, die deutsche Verfassungsidentität zu wahren, bedarf keiner näheren Begründung. Auf die verfassungsrechtlichen Bedenken wurde im 41. Tätigkeitsbericht hingewiesen. Die deutschen Verhandlungsteilnehmer unterliegen ferner einer dauerhaften Integrationsverantwortung. Diese ist darauf gerichtet, bei der Übertragung von Hoheitsrechten und bei der Ausgestaltung der europäischen Entscheidungsverfahren dafür Sorge zu tragen, dass in einer Gesamtbetrachtung sowohl das politische System der Bundesrepublik Deutschland als auch das der Europäischen Union demokratischen Grundsätzen im Sinne des Art. 20 Abs. 1 und Abs. 2 in Verbindung mit Art. 79 Abs. 3 GG entspricht (BVerfG Urteil vom 30. Juni 2009 – 2 BvE 2,5/08 u. a., – BVerfGE 123, 267, 365; zur Integrationsverantwortung allgemein Schmahl, Singuläre Integrationsverantwortung des Parlaments – oder kumulative Integrationsverantwortung der Parlamente?, DÖV 2014, 501). Die deutschen Verhandlungsteilnehmer haben sich daher immer der Rückwirkungen der unionsrechtlichen Reformvorschläge auf das die Verfassung konkretisierende (Fritz Werner, Verwaltungsrecht als konkretisiertes Verfassungsrecht, DVBl. 1959, 527) nationale Datenschutzrecht zu vergewissern. Die Auswirkungen des Verordnungsvorschlags auf das Datenschutzrecht jedenfalls im öffentlichen Bereich sind indessen unübersehbar (vgl. Herrmann, Anmerkungen zur Reform des europäischen Datenschutzrechts, ZD 2014, 439). Es trifft zwar zu, dass nicht alle Mitgliedstaaten der EU formal einen öffentlichen und einen nicht-öffentlichen Bereich unterscheiden. Daher liegt es nahe, unionsrechtlich die Unterscheidung im Interesse einer Vollharmonisierung zu ignorieren. Die Unterscheidung darf aber nicht mit der in der Tat nicht in allen Mitgliedstaaten bestehenden Trennung von öffentlichem und privatem Recht verwechselt werden. Materiell ist in allen Mitgliedstaaten ein Sonderrecht für die Staatstätigkeit, namentlich die Verwaltung, geboten. Für die Bundesrepublik Deutschland folgt das aus dem Gewaltenteilungsprinzip als tragendem Element des Rechtsstaats (BVerfG, Urteil vom 17. Juli 1984 – 2 BE 11,

15/83 –, BVerfG 67, 102, 130). Das bedeutet, dass der Anwendungsvorrang des Unionsrechts nicht bundes- oder landesrechtliche Regelungen verdrängen darf, die den spezifischen (Datenschutz-)Belangen der einzelnen Sachgebiete des öffentlichen Bereichs Rechnung tragen. Eine die deutsche horizontale und vertikale Gewaltenteilung reflektierende Subsidiaritätsklausel wie § 1 Abs. 3 BDSG fehlt jedoch im Verordnungsvorschlag. Ungeachtet der Frage, ob nicht schon nur eine Richtlinie mit entsprechenden Freiräumen zulässig wäre, müsste der Anwendungsvorrang der DSGVO dergestalt zurückgenommen werden, dass eine nationale besondere Datenschutzgesetzgebung zur Ermöglichung eines höheren Schutzniveaus der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen in Ausübung ihrer hoheitlichen Aufgaben zulässig bleibt.

1.1.4
Rechtsprechung

1.1.4.1
Europäischer Gerichtshof

Einen Bericht über die Rechtsprechung des EuGH geben Schwartmann und Theodorou (Aktuelle Rechtsprechung des EuGH zum Datenschutzrecht, RDV 2014, 61). Der EuGH traf im Berichtszeitraum einige wegweisende Entscheidungen. An erster Stelle zu nennen ist das Urteil vom 8. April 2014 (C-293/12 – Digital Rights Ireland u. C-Seitlinger u. a. –, DÖV 2014, 617 m. Anm. Heinrich Amadeus Wolff = EuZW 2014, 459 = MMR 2014, 412 = NJW 2014, 216 = NVwZ 2014, 709 = RDV 2014, 148; hierzu die Anm. von Petri, ZD 2014, 300 und Kunert DÖV 2014, 103 ff. und die Besprechungen von Simitis, Die Vorratsdatenspeicherung – ein unverändert zweifelhaftes Privileg NJW 2014, 2158; Kühling. Der Fall der Vorratsdatenspeicherungs-RL und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, 681; Priebe, Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH, EuZW 2014, 456 ff.; Boehm/Cole, Studie zu den Folgen des EuGH-Urteils zur Vorratsdatenspeicherung – Auswirkungen auf Mitgliedstaaten, EU-Rechtsakte und internationale Abkommen, ZD 2014, 553, ferner Roßnagel, MMR 2014, 372; Streinz, JuS 2014, 758). Die Große Kammer des EuGH erklärte darin die RL 2006/24/EG vom 15. März 2006 (ABl. 2006 L105, 54) für ungültig. Die Richtlinie greife in Art. 7 und 8 GRCh ein, weiche von der RL 55/46/EG und der RL 2002/58/EG ab und verletze den Grundsatz der Verhältnismäßigkeit. Das bedeutet kein absolutes Verdikt der Vorratsdatenspeicherung. Wie schon Simitis zutreffend betonte, geht der EuGH von der prinzipiellen Zu-

lässigkeit der Vorratsdatenspeicherung aus. Durch die verkürzte zweigliedrige Prüfung des Verhältnismäßigkeitsgrundsatzes (ebenso etwa EuGH vom 9. November 2010 – C-92/09 und C-93/09 m. Anm. Volker und Markus Schecke, NJW 2011, 1338 Tz. 74), bei der Erforderlichkeit und Angemessenheit vermengt werden, entstand der Eindruck, die konkret unangemessene Vorratsdatenspeicherung lasse die Erforderlichkeit der Vorratsdatenspeicherung generell entfallen. Eben dies hat der EuGH aber gerade nicht entschieden. Nach deutscher Rechtstradition besteht der Grundsatz der Verhältnismäßigkeit aus drei Teilgeboten, nämlich dem Gebot der Geeignetheit, der Erforderlichkeit und der Angemessenheit (Reichold/Kühl/Ronellenfitsch, Einführung in die Rechtswissenschaft, 2. Aufl. 2014, § 27 Rdnr. 22). Eine unangemessene Maßnahme kann folglich durchaus noch erforderlich sein. In bestimmten Konstellationen kann die erforderliche Maßnahme auch angemessen sein. So verhält es sich bei der Vorratsdatenspeicherung. In Ausnahmesituationen kommt weiterhin die Vorratsdatenspeicherung in Betracht. Dass dann auch die Vorgaben von BVerfG, Urteil vom 2. März 2010, 1 BvR 256, 263, 586/08, BVerfGE 125, 260 zu beachten sind, versteht sich von selbst.

Nicht weniger bedeutsam ist die Google-Entscheidung des EuGH vom 13. Mai 2014 (C-131/12- Google Spain ./. AEPD, AfP 2014, 245 = BeckRS 2014, 80862 = DuD 2014, 559 = GRUR 2014, 895 = EuGRZ 2014, 320 = EuZW 2014, 541 = EWS 2014, 166 = JZ 2014, 1009 = K & R 2014, 502 = MMR 2014, 455 = NJW 2014, 2257 = NJ 2014, 379 = NVwZ 2014, 857 = RiW 2014, 433 = WRP 2014, 805. Hierzu die Anmerkungen von Sörup, MMR 2014, 463; Karg, ZD 2014, 359 und Streinz, JuS 2014, 1140; ferner Nolte, Das Recht auf Vergessenwerden – mehr als nur ein Hype?, NJW 2014, 2238, Kreile/Thalhofer, Suchmaschinen und Pluralitätsanforderungen, ZUM 2014, 629; Kühling, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, 527; Kühling/Klar, Löschpflichten vs. Datenaufbewahrung – Vorschläge zur Auflösung eines Zielkonflikts bei möglichen Rechtsstreitigkeiten, ZD 2014, 506; Ziebarth, Google als Geheimnishüter? – Verantwortlichkeit der Suchmaschinenbetreiber nach dem EuGH-Urteil, ZD 2014, 394; Boehme-Neßler, Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 2014, 825; Beyvers/Herbrich, Das Niederlassungsprinzip im Datenschutzrecht – am Beispiel von Facebook – Der neue Ansatz des EuGH und die Rechtsfolgen, ZD 2014, 558). Die Entscheidung, die in Abweichung zum Schlussantrag des Generalanwalts (BeckRS 2013, 8134 Tz. 18) erging, wurde vielfach missverstanden. Ein (absurdes) Recht auf Vergessen, d. h. auf Vergessenwerden, wurde nicht thematisiert, geschweige denn anerkannt. Anerkannt wurde ein Recht, nicht mit Hilfe von Suchmaschinen gefunden zu werden.

Hierzu war die Feststellung nötig, dass die Tätigkeit des Suchmaschinenanbieters ggf. eine eigenständige, von ihm zu verantwortende Verarbeitung personenbezogener Daten darstellt, sodass eine Verlinkung zu – selbst rechtmäßigen – Inhalten eine selbstständige Persönlichkeitsrechtsverletzung darstellen kann. Der Suchmaschinenanbieter benötigt daher eine Erlaubnis für die Datenverarbeitung. Diese kann sich aus Art. 7 lit. f RL 95/46/EG ergeben. Erforderlich ist dann aber eine Interessenabwägung, in die man beispielsweise das Interesse des Straftäters auf Verschwinden aus dem öffentlichen Bewusstsein mit dem Recht des Opfers, im öffentlichen Gedächtnis präsent zu bleiben, einstellen kann. Überwiegen die Interessen des von seiner Erwähnung im Internet negativ Betroffenen, ist der Suchmaschinenanbieter auf dessen Antrag verpflichtet, den Link aus dem Suchergebnis zu löschen. Die Entscheidung ist materiellrechtlich nicht so spektakulär wie vielfach getan wird. Bedeutsamer ist der formelle Aspekt, dass es sich bei der Niederlassung von Google in Spanien (Google Spain) um eine Niederlassung i. S. d. Art. 4 Abs. 1 lit. A der RL 95/46/EG handle.

Für die Unabhängigkeit der Datenschutzbeauftragten der Mitgliedstaaten ist es eine begrüßenswerte Bestärkung, dass der EuGH mit Urteil vom 8. April 2014 (C-288/12 – Kommission/Ungarn, ZD 2014, 301) entschied: „Ungarn hat dadurch gegen seine Verpflichtungen aus der RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verstoßen, dass es das Mandat der Kontrollstelle für den Schutz personenbezogener Daten vorzeitig beendet hat.“ Damit knüpft der EuGH an seine frühere Rechtsprechung an (Urteil vom 9. März 2010 – Rs. C-518/07 – Slg. I 2010, 1897; Urteil vom 16. Oktober 2012 – C-614/10 –, ZD 2012, 563). Zu betonen ist, dass sich nach Ansicht des EuGH das Erfordernis, die Einhaltung der Unionsvorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch eine unabhängige Stelle zu überwachen, aus dem Primärrecht der Union, nämlich aus Art. 8 Abs. 3 der GRCh und aus Art. 16 Abs. 2 AEUV, ergibt. Einen weiten Begriff der personenbezogenen Daten propagiert zu Recht das Urteil vom 17. Juli 2014 (C-141/12 und C-372/12 – ZD 2014, 515). Danach ist Art. 2 lit. a der RL 95/46/EG dahin auszulegen, dass es sich zum einen bei den Daten über denjenigen, der einen Aufenthaltstitel beantragt, die in einer „Entwurfsschrift“ wiedergegeben sind, um „personenbezogene Daten“ handelt. Ob das generell für alle Entwürfe nach den Gesetzen der Mitgliedstaaten gilt, muss bezweifelt werden.

1.1.4.2
Bundesverfassungsgericht

Im Berichtszeitraum sind nur Kammerbeschlüsse zu verzeichnen. Der datenschutzrechtliche Aspekt der sozialrechtlichen Regelbedarfsberechnung klingt im Beschluss vom 23. Juli 2014 (1 BvL 10/12, 1 BvL 12/12, 1 BvR 1691/13 – NJW 2014, 3425) an. In einem Verfahren über die Verpflichtung zur Auskunft über sexuelle Beziehungen aus einer Zeit, in der die Antragstellerin nicht verheiratet war und nur in einer „lockeren" Beziehung gelebt hat, ist nach dem Beschluss vom 3. März 2014 (1 BvR 472/14, NZFam 2014, 405) das allgemeine Persönlichkeitsrecht der Antragstellerin zu beachten. Die drohenden Nachteile eines irreparablen Eingriffs in das Recht auf informationelle Selbstbestimmung können es gebieten, die Sichtung und Auswertung der im Rahmen eines Ermittlungsverfahrens wegen des Verdachts des Besitzes kinderpornographischer Schriften (§ 184b StGB) sichergestellten Beweisgegenstände bis zur Entscheidung über die Verfassungsbeschwerde vorläufig zu untersagen, wenn dadurch der staatliche Strafanspruch zwar verzögert, nicht aber vereitelt wird; so der Beschluss vom 5. Februar 2014 (2 BvR 200/14, NVwZ 2014, 136).

1.1.4.3
Bundesverwaltungsgericht

Nach dem Urteil vom 21. Januar 2014 (BVerwG 6 B 43.13, ZD 2014, 483) unterliegen Angaben, die ein Unternehmen im Rahmen eines Antrags auf Zulassung zu einem Frequenzversteigerungsverfahren zu seinem Frequenzbedarf macht, dem Schutz als Betriebs- und Geschäftsgeheimnis. Laut Beschluss vom 19. März 2014 (6 P 1.13, NZA 2014, 860 = NZA-RR 2014, 387) kann der Personalrat nicht verlangen, dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden; seine Überwachungsaufgabe kann er bereits effektiv wahrnehmen, wenn er zunächst nur die anonymisierten Arbeitszeitlisten der Dienststelle erhält.

1.1.4.4
Bundesgerichtshof

In dem vielbeachteten Urteil vom 28. Januar 2014 (VI R 156/13, BGHZ 200, 38 = DB 2014, 588 = MIR 2014, Dok. 025 = MMR 2014, 489 = NJW 2014, 1235 m. Anm. Schulte am Hülse/Timm = NVwZ 2014, 747 m. Anm. Kirchberg = RDV 2014, 154 m. Anm. Joos = WM 2014, 452 = ZD 2014, 306 = ZIP 2014, 476) entschied der BGH, dass die Scoringformel im Rahmen einer

von der SCHUFA zu erteilenden datenschutzrechtlichen Auskunft geheim bleiben darf. Das rief einen Sturm der Empörung hervor, entspricht aber meiner Aufsichtspraxis, was in einer auf der Homepage des HDSB wiedergegebenen Presseerklärung vom 30.01.2014 erläutert wurde.

Immer wieder rechtliche Schwierigkeiten bereiten Portale. Häufig werden Portale missbraucht, um die Verärgerung über Lehrer, Ärzte u. dgl. in polemischer unsachlicherer Weise abzureagieren. Soweit die Grenze zur Schmähkritik nicht überschritten wird, können sich die Betroffenen nur wehren, wenn ihnen der Verletzer bekannt ist. Der Betreiber von Internet-Portalen ist indessen gem. § 12 Abs. 2 TMG nicht berechtigt, die zur Bereitstellung des Telemediums erhobenen Anmeldedaten herauszugeben (Urteil vom 1. Juli 2014 – VI ZR 345/13, NJW 2014, 2652).

Nach dem Urteil vom 22. Januar 2014 [(I ZR 218/12 – RDV 2014, 159 (Ls)] ist Datenerhebung bei Minderjährigen zu Werbezwecken unzulässig. Die Pflicht zur unverzüglichen Löschung aufgezeichneter Telefonate ist Gegenstand des Beschlusses vom 18. Februar 2014 (StB 8/13, AnwBl 2014, 357 = BRAK-Mitt. 2014, 148 = BeckRS 2014, 04893 = NJW 2014, 1314 m. Anm. Roggan = NStZ-RR 2014, 149 = StV 2014, 388 = wistra 2014, 278). Nach dem Urteil vom 3. Juli 2014 (III ZR 391/13, BeckRS 2014, 14643 = K&R 2014, 593 = NJW 2014, 2500 = ZD 2014, 461 m. Anm. Eckhardt = ZUM-RD 2014, 621) sind die Erwägungen des EuGH zur Ungültigkeit der RL über die Vorratsspeicherung von Daten auf die siebentägige Speicherung von IP-Adressen zu den in § 100 Abs. 1 TKG bestimmten Zwecken nicht übertragbar (vgl. auch Breyer: Personenbezug von IP-Adressen – Internetnutzung und Datenschutz, ZD 2014, 400).

1.1.4.5
Bundesarbeitsgericht

Erwähnenswert ist der Beschluss vom 10. Dezember 2013 (1 ABR 43, 12, DuD 2014, 633) zur Mitbestimmung des Betriebsrats beim Einsatz eines Routenplaners zu Abrechnungszwecken. Für den Auskunftsanspruch nach § 34 BDSG hat der Beschluss vom 3. Februar 2014 (DB 2014, 728 = NJW 2014, 1408) den Rechtsweg zu den Arbeitsgerichten eröffnet. In einer Betriebsvereinbarung kann bestimmt werden, dass über einen Zufallsgenerator ausgewählte Arbeitnehmer beim Verlassen des Betriebsgeländes kontrolliert werden. Das zulässige Maß der damit verbundenen Beschränkung des allgemeinen Persönlichkeitsrechts der Arbeitnehmer zu Gunsten schützenswerter Belange des Arbeitgebers richtet sich nach dem Grundsatz der Verhältnismäßigkeit. Der Beschluss vom 15. April 2014 (1 ABR 2/13, AuR

2014, 247 L = BeckRS 2014, 68694 = DB 2014, 1208 L = FD-ArbR 2014, 358239 = MDR 2014, 906 = NZA 2014, 551 = RDV 2014, 272 = ZD 2014) behandelt eine Betriebsvereinbarung, die unter Beachtung von § 75 Abs. 2 BetrVG Kontrollen der Arbeitnehmer beim Verlassen des Betriebsgeländes anordnet, als Rechtsvorschrift i. S. d. § 4 Abs. 1 BDSG, die sowohl die automatisierte als auch die nicht automatisierte Erhebung, Nutzung oder Verarbeitung personenbezogener Daten von Arbeitnehmern erlaubt.

1.1.4.6
Bundessozialgericht

Nach dem Urteil vom 2. April 2014 (B 6 KA 19/13 R, openJur 2014, 16680) haben die kassen-(zahn-)ärztlichen Vereinigungen den Krankenkassen die (Zahn-)Arztnummer in unverschlüsselter Form zu übermitteln. Dies ergebe sich bereits aus dem systematischen Zusammenhang der Regelungen in § 295 Abs. 2 SGB V und § 293 Abs. 4 SGB V. Dort sei ausdrücklich bestimmt, dass die von der Kassen-(zahn-)ärztlichen Bundesvereinigung [K(Z)ÄB] zu führenden Verzeichnisse der an der vertragsärztlichen Versorgung teilnehmenden Ärzte bzw. Zahnärzte u. a. die Angabe der „Arzt- oder Zahnarztnummer (unverschlüsselt)“ zu enthalten hätten. Das Gesetz enthalte an vielfältiger Stelle Regelungen über eine die Arztnummer betreffende Datenerhebung bzw. -übermittlung. In keiner dieser Normen finde sich ein zusätzlicher Hinweis darauf, dass die Daten verschlüsselt oder unverschlüsselt zu verarbeiten oder zu übermitteln seien. Bei der Grundnorm des § 293 Abs. 4 SGB V sei das nicht der Fall.

1.1.4.7
Bundesfinanzhof

Unter dem Aktenzeichen VIII R 8/12 ist immer noch ein Revisionsverfahren anhängig, in welchem folgende Fragen zu klären sind:

1. Ist die Tätigkeit eines Steuerpflichtigen, der über keinen Studienabschluss verfügt, mit der eines Wirtschaftsinformatikers nur dann vergleichbar und folglich nicht als gewerbliche, sondern als freiberufliche Tätigkeit i. S. d. § 18 Abs. 1 Nr. 1 EStG anzusehen, wenn der Steuerpflichtige über vergleichbare Kenntnisse nicht nur im IT-Bereich und seinem speziellen Tätigkeitsbereich, sondern auch in Englisch, Mathematik, Statistik, Operations Research, Grundlagen der BWL und VWL, Buchführung und Bilanzierung, Kostenrechnung und Leistungsrech-

nung, Produktionswirtschaft, Finanzwirtschaft und Investitionswirtschaft, Marketing, Controlling, Produktion und Logistik, DV-Recht und Datenschutz sowie des Wirtschaftsrechts verfügt?

2. Muss ein von dem Kläger beantragter Beweis in Form einer Wissensprüfung erst dann erhoben werden, wenn der Kläger hinreichend darlegt, dass er Kenntnisse in allen Hauptbereichen des Studiums der Wirtschaftsinformatik erworben hat und diese entweder durch geeignete Fortbildungsveranstaltungen oder praktische Arbeiten nachweist?

1.1.4.8
Staats- und Verfassungsgerichtshöfe der Länder

Den Aspekt des Überwachungsdrucks betont der VerfGH Berlin hinsichtlich der Ermächtigung der Polizei zur Abfertigung von Übersichtsaufnahmen (Urteil vom 11. April 2014 – 129/13, DVBl. 2014, 922). Die Verwertung rechtswidrig und strafbar erlangter Steuerdaten-CDs erklärte der VerfGH RhPf im Urteil vom 24. Februar 2014 (B 26/13, NJW 2014, 1434, hierzu Selmer JuS 2014, 1952) für zulässig. Damit wurde dem populistischen Argument Rechnung getragen, die Bekämpfung von Steuersünden entfalte eine größere Verhaltenssteuerung als die negative Vorbildwirkung einer Kollaboration mit Rechtsbrechern. Die Rechtsprechung untergräbt die Rechtstreue der Bürgerinnen und Bürger; (kritisch auch Hamm, NJW Heft 7/2010 editorial, Kämmerer, NJW-aktuell Heft 7/2010, A.12). Nach dem Urteil des LVG LSA vom 25. September 2014 (LVG 9/13) besteht eine Landesgesetzgebungskompetenz, soweit die Gefahrenabwehr und nicht die vorbeugende Strafverfolgung den Hauptzweck einer Regelung darstellt. Die einfachgesetzlichen Konsequenzen sind ausführlich dargestellt in Pietzner/Ronellenfitsch, Das Assessorexamen im Öffentlichen Recht, 13. Aufl. 2014, Rdnr. 165.

1.1.4.9
Rechtsprechung in Hessen

Mit Beschluss vom 2. Januar 2014 (10 B 1397/13 –, openJur 2014, 2772) hat der HessVGH die hier vertretene Auslegung von § 35 Abs. 4a BDSG bestätigt. Nach dem Beschluss vom 22. Juli 2014 (22 A 2226/13.PV – openJur 2014, 19752) erstreckt sich das Mitbestimmungsrecht des Personalrats nach § 74 Abs. 1 Nr. 3 HPVG nicht auf die Bestellung des Vertreters des behördlichen Datenschutzbeauftragten gemäß § 5 Abs. 1 S. 1 HDSG. Die Regelungen zum Schutz von Sozialdaten im Vierten Kapitel des Achten Buchs Sozialgesetzbuch sind nach dem Urteil des HessVGH vom 16. September 2014 (10 A 500/13 – openJur 2014, 10696) im Rahmen ihres Anwendungs-

bereichs für die Tätigkeit der Träger der öffentlichen Jugendhilfe gegenüber den allgemeinen Bestimmungen im Ers-ten und Zehnten Buch Sozialgesetzbuch sowie den Regelungen in den Datenschutzgesetzen des Bundes und der Länder vorrangig anzuwenden. Dies gilt sowohl für hierin enthaltene Einschränkungen als auch für Erweiterungen gegenüber den allgemeinen Datenschutzbestimmungen. Die Fremderhebung von Sozialdaten durch ein Jugendamt ist nur unter den Voraussetzungen des § 62 Abs. 3 SGB VIII zulässig, soweit nicht die Sonderregelung in § 68 SGB VIII eingreift. Das VG Wiesbaden verurteilte mit Entscheidung vom 21. Januar 2014 (7K 898/13.WI) den beklagten Magistrat einer Stadt, der Klägerin einer Fraktion der Stadtverordnetenversammlung eine gemäß § 43 HGO gegenüber der Stadtverordnetenversammlung gestellte Anfrage „Welche Kosten hat der Neubau anstelle des A-Hauses inklusive Grundstückserwerb insgesamt verursacht“ zu beantworten. Zur Begründung führte das VG aus, dass das Auskunftsrecht bei Aufeinandertreffen der Kontrollfunktion/den Kontrollrechten der Gemeindevertretung mit dem Steuergeheimnis und mit datenschutzrechtlichen Vorschriften Vorrang genieße. Nach VG Wiesbaden, Urteil vom 28. Februar 2014 (6 K 152/ 14.WI.A, InfAuslR 2014, 237), führt das Bundesamt für Migration und Ausländer keine ordnungsgemäßen elektronischen Akten. Abgemildert wurde diese Entscheidung durch Urteil vom 26. September 2014 (6 K 691/ 14.WI.A). Das VG Gießen entschied durch Beschluss vom 9. Januar 2014 [(3 L 2627/13.GI, DVBl 2014, 397 = LSK 2014, 120425 (Ls.)], dass einem Studierenden nicht das Recht zustehe, Einsicht in die Buchführungs- und Haushaltsunterlagen des AStA oder des Studierendenparlaments zu nehmen und diese zu prüfen. Laut VG Frankfurt, Urteil vom 28. Juli 2014 (23 – K 1741 14 F./PV.– BeckRS 2014, 5225), kann ein Personalrat aufgrund von § 62 Abs. 2 S. 1 HPVG verlangen, über die im Einzelnen gewährten Leis-tungsprämien, die Begründungen dieser Leistungsprämien und die Grundlagen der Leistungsfeststellungen unterrichtet zu werden. Die Vorschrift enthält eine abschließende personalvertretungsrechtliche Konkretisierung des Datenschutzes und der Eingriffsbefugnisse in das Recht auf informationelle Selbstbestimmung. Passend zu dem auf der Homepage des HDSB abrufbaren Beitrag „Mobilität unter Aufsicht – Freie Fahrt und jeder weiß wohin“ erging das Urteil des LG Kassel vom 25. Februar 2014 (1 S 172/13, ZD 2014, 363), in welchem zutreffend ausgeführt wurde, dass durch den aus Kfz-Kennzeichen, Fahrzeugidentifikationsnummer und Datum des Schadensfalls bestehenden Datensatz die Person des Fahrzeughalters bestimmbar werde, sodass es sich um personenbezogene Daten handele. Eine geschäftsmäßige Erhebung und Speicherung von Daten liege auch bei brancheninternen Warndiensten wie etwa dem HIS (Hinweis- und Informationssystem der Versicherer) vor. Schutzwürdige Interes-

sen des Betroffenen am Ausschluss von Erhebung und Speicherung der Daten lägen aber nicht vor. Demgegenüber bestehe ein nicht unerhebliches Interesse der Versicherungswirtschaft, Betrugsverhalten bei der Mehrfachnennung im Falle fiktiver Schadensabrechnung zu verhindern. Die Versicherungswirtschaft sei nicht verpflichtet, zur Durchführung der Interessenabwägung statistische Erhebungen über die Effektivität des Informationssystems anzustellen. Die HIS-Auskunftei sei geeignet, den mit ihr verfolgten Zweck der Eindämmung von Betrugsverhalten im Zusammenhang mit der fiktiven Abrechnung von Schadensfällen zu erreichen. Die Erforderlichkeit der Speicherung ergebe sich daraus, dass es keine objektiv zumutbare Alternative gibt. Dem ist zuzustimmen. Die Ermächtigung zur Datenspeicherung ist ebenfalls zutreffend auf § 29 BDSG gestützt.

1.1.4.10
Sonstige Rechtsprechung

Auf die Probleme der Videoüberwachung wird unter Ziff. 5.2.1 ausführlich eingegangen. Zu erwähnen ist hier noch das Urteil des NdsOVG vom 29. September 2014 (11 LC 114/13, DVBl 2014, 1464) zur Videoüberwachung von Eingangsbereich und Treppenaufgängen eines privaten Bürogebäudes, das die in Hessen zugelassene Praxis bestätigt. Eher kurios ist die Entscheidung des OLG Koblenz vom 15. Januar 2014 (5 U 1243/13 – ZD 2014, 19), deren Leitsatz lautet: „Bringt ein Gast den weiteren Betrieb eines Bordells durch Werfen von Stinkbomben zum Erliegen, was den Bordellbetreiber veranlasst, zur Identitätsklärung die Videoaufzeichnung der Tat im Internet zu veröffentlichen, muss dies beendet werden, sobald die Personalien des Täters feststehen.“ Von datenschutzrechtlich relevanten Stinkbombenanschlägen auf hessische Bordelle ist nichts bekannt.

1.1.5
Publikationen

Als Nachtrag zum vorangegangenen Tätigkeitsbericht ist hinzuweisen auf Roos/Buchmüller, Die Entwicklung des Datenschutzrechts im Jahr 2013 – Beitrags- und Rechtsprechungsübersicht, ZD 2014, 167. Einen kursorischen Überblick über die Entwicklung des Datenschutzrechts im ersten Halbjahr 2014 geben Gola und Klug NJW 2014, 2622.

Die Probleme von Big Data behandeln Ohrtmann und Schwierig, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984; Götz, Big Data und der Schutz von Datenbanken – Überblick und Grenzen, ZD 2014, 563; Arning/Moos, Big Data bei verhaltensbe-

zogener Online-Werbung – Programmatic Buying und Real Time Advertising, ZD 2014, 242 und Martini, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481. Im Übrigen befassen sich datenschutzrechtliche Beiträge mit der Beschäftigtenüberwachung (Hornung/Knieper, ZD 2014, 383), den Datenschutzbeauftragten (Bittner, RDS 2014, 183), dem Personenbezug dynamischer IP-Adressen (Specht/Müller-Riemenschneider, ZD 2014, 71), den Datenschutzerklärungen bei der Verwendung von Cookies (Stiemerling/Lachenmann, ZD 2014, 133), der Online-Werbung (Arning-Moos, ZD 2014, 126, 242), der Vereinbarkeit von Dash-Cams mit datenschutzrechtlichen Grundsätzen (Knyrim/Trieb, ZD 2014, 547) sowie mit Stadionverboten (Müller-Eiselt, DVBl 2014, 1168). Zur Analyse des Fahrverhaltens mit Hilfe der Telematik und Bordelektronik äußern sich Kinast/Kühnl, NJW 2014, 3057.

Die Problematik sozialer Netzwerke behandeln Beyvers/Herbrich: Das Niederlassungsprinzip im Datenschutzrecht – am Beispiel von Facebook – Der neue Ansatz des EuGH und die Rechtsfolgen (ZD 2014, 558).

1.1.6
Datenschutzbewusstsein

Auf den Wandel im Datenschutzbewusstsein der „Generation Facebook“ gegenüber der „Generation Volkszählung“ (vgl. Cap, „Sicher oder nur scheinbar sicher? Informatik-Systeme und ihre Folgen“, Forschung und Lehre, 2014, 958) wurde bereits in früheren Tätigkeitsberichten aufmerksam gemacht. Die „Mitteilungssucht“ sämtlicher Präferenzen ist vielfach derart gestiegen, dass die informationelle Selbstbestimmung ihren Schwerpunkt von der Privatheit auf die (positive und negative) Informationsfreiheit zu verlagern droht. Die Entwicklung zum Cookie-Pricing, den „Black Boxes“ und „Smart Grits“ lässt sich kaum aufhalten. Demgegenüber ist gleichwohl zu betonen, dass die Gewährleistung der Privatheit nicht nur verfassungsrechtlich geboten, sondern auch anthropologisch unverzichtbar ist. Der Mensch ist zwar ein Gemeinschaftswesen (Zoon politikon), das anderer Menschen bedarf, um seine Individualität entfalten zu können. Er benötigt aber auch einen Rückzugsraum, in dem er unbeobachtet „für sich selbst“ sein kann. Nach Reichhoff, Ichbezogen, eingebunden und überwacht, Forschung und Lehre 2014, 956, erschufen die Herrschenden die Götter, die alles sahen. Durch die technische Entwicklung sei das immer wachende Auge der Götter Wirklichkeit geworden. „Deshalb brauchen wir Abschirmmaßnahmen, um wenigstens einen Rest von Privatheit zu retten.“ Die Abschirmmaßnahmen sind vor allem rechtliche Regulierungen.

1.2
Rechtsentwicklung in Europa

Auf europäischer Ebene wurde mit dem Vorschlag der Europäischen Kommission für eine Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vom 7. Februar 2013 ein Gesetzgebungsverfahren eingeleitet, das bei der anschließend zu würdigenden Novellierung des BSI-Gesetzes nicht ignoriert werden darf. Die vorgeschlagene Richtlinie enthält verbindliche zu erreichende Ziele (Art. 288 Abs. 2 AEUV), die teilweise so detailliert sind, dass praktisch kein Umsetzungsspielraum für die Mitgliedstaaten mehr besteht. Aus der Verbindlichkeit des Richtlinienziels folgt, dass die Mitgliedstaaten verpflichtet sind, alle erforderlichen Maßnahmen zu ergreifen, um die vollständige Wirksamkeit der Richtlinie entsprechend ihrer Zielsetzung zu gewährleisten. Das Institut der „unmittelbaren Wirksamkeit“ von Richtlinien betrifft zwar nur die Rechtswirksamkeit bereits erlassener Richtlinien vor Umsetzung, so dass Richtlinienentwürfe keine zwingende Vorwirkung entfalten. Trotzdem wäre es gemeinschaftswidrig, vor Erlass der im Entwurfsstadium befindlichen Richtlinie eine rechtliche oder tatsächliche Situation zu schaffen, die das aktuelle Verfahren zum Scheitern bringen könnte. Anliegen der vorgeschlagenen Richtlinie ist die Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS). Hierbei geht es um die Erhöhung der Sicherheit des Internets und der privaten Netze und Informationssysteme, die für das Funktionieren unserer Gesellschaften und Volkswirtschaften unverzichtbar sind. Dies soll erreicht werden, indem die Mitgliedstaaten verpflichtet werden, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit untereinander zu verbessern, und indem die Betreiber kritischer Infrastrukturen wie Energieversorger, Verkehrsunternehmen und wichtige Anbieter von Diensten der Informationsgesellschaft (Plattformen für den elektronischen Geschäftsverkehr, soziale Netze usw.) und die öffentlichen Verwaltungen verpflichtet werden, geeignete Schritte zur Beherrschung von Sicherheitsrisiken zu unternehmen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden.

1.3
Rechtsentwicklung in Deutschland

Datenschutzrechtlich relevante Regelungen finden sich in der Verordnung zur Erhebung von Gebühren und Auslagen für die Bereitstellung von Daten nach den Regelungen der Datentransparenzverordnung (Datentransparenz-Gebührenverordnung – DaTraGebV) vom 15. Mai 2014 (BGBl. I S. 458),

im Achten Gesetz zur Änderung des Zweiten Buches Sozialgesetzbuch – Ergänzung personalrechtlicher Bestimmungen vom 4. August 2014 (BGBl. I S. 1306), in der Neufassung des Umweltinformationsgesetzes vom 5. November 2014 (BGBl. I S. 1643), im Gesetz zur Änderung des Umweltstatistikgesetzes und des Wasserhaushaltsgesetzes vom 20. November 2014 (BGBl. I S. 1724), im Gesetz zur Änderung des Gesetzes zur Fortentwicklung des Meldewesens vom 25. November 2014 (BGBl. I S. 1738) und im Gesetz zur Änderung des Straßenverkehrsgesetzes, der Gewerbeordnung und des Bundeszentralregistergesetzes vom 4. Dezember 2014 (BGBl. I S. 1802).

1.4
Besonderheiten, Arbeitsschwerpunkte und Statistik

1.4.1
Wiederwahl – Hauptamtliche Ausübung des Amtes

Seit dem 18. September 2003 bin ich Hessischer Datenschutzbeauftragter. Ich hatte bisher das Amt als Nebenamt neben meiner ordentlichen Professur in Tübingen ausgeübt und war bereits zweimal vom Hessischen Landtag einstimmig wiedergewählt worden. Nach der mit der Änderung des Hessischen Datenschutzgesetzes vom 20. Mai 2011 verbundenen Übertragung der Aufgaben der Aufsichtsbehörde für den nicht-öffentlichen Bereich auf den Hessischen Datenschutzbeauftragten war die Ausübung im Nebenamt nur noch als Übergangslösung für die laufende Amtsperiode vorgesehen. Mit Beginn der 19. Legislaturperiode des Hessischen Landtags und der dann vorgesehenen Wahl war das Amt als Hauptamt auszuüben. Ich habe daher meinen Lehrstuhl aufgegeben, um mich ganz dem Amt als Hessischer Datenschutzbeauftragter widmen zu können.

Am 12. März 2014 hat mich der Hessische Landtag einstimmig auf Vorschlag der Landesregierung nunmehr als hauptamtlichen Datenschutzbeauftragten wiedergewählt.

1.4.2
Räumliche Konsolidierung der Dienststelle

Im Hinblick auf die räumliche Unterbringung der Dienststelle bestand im Berichtszeitraum folgende Situation.

Die Hauptfläche der Dienststelle befand sich im Delta-Haus. Der Mietvertrag für diese Fläche lief bis März 2017. Der aus der Übertragung der Aufgabe der Aufsichtsbehörde für den nicht-öffentlichen Bereich auf den Hes-

sischen Datenschutzbeauftragten resultierende zusätzliche Flächenbedarf wurde durch zusätzliche Anmietung von Flächen im Nebengebäude des Delta-Hauses, der Rotunde, auf der Grundlage eines Zwei-Jahres-Vertrages gedeckt, der zum April 2014 auslief. Dabei handelte es sich um eine Übergangslösung, die weitergehende Bemühungen um eine möglichst einheitliche Unterbringung der Dienststelle erforderlich machte. Da der Vermieter der Flächen im Delta-Haus nicht bereit war, den Hauptmietvertrag zu beenden, im Hauptgebäude des Delta-Hauses aber Mietflächen frei wurden, konzentrierten sich die Bemühungen auf eine längerfristige dortige Unterbringung der Dienststelle. Nach langwierigen Verhandlungen konnte schließlich eine wirtschaftliche Mietlösung unter Einbeziehung des Hauptmietvertrages mit der Anmietung einer weiteren Etage, einer Verbesserung des bisherigen Mietverhältnisses und einer einheitlichen Mietdauer für die gesamte Fläche erreicht werden.

Auf diese Weise konnte insbesondere auch kostengünstig eine bessere Ausfallsicherheit der internen IT realisiert werden.

Beeinträchtigungen der Arbeit entstanden durch Umbauarbeiten und Renovierungen in der bisherigen Mietfläche, die Interimsumzüge u. a. von zentralen Serviceeinheiten notwendig machten, den Umzug der bisher in anderen Räumlichkeiten untergebrachten Beschäftigten infolge der Renovierungsarbeiten und die umfangreichen Änderungen an der internen IT und Verkabelung. Die Planungs- und Begleitungsarbeiten für eine reibungslose Abwicklung nahmen erhebliche Personalkapazitäten in Anspruch (insgesamt 920 Personenstunden), die dem operativen Geschäft naturgemäß fehlten.

1.4.3
Arbeitsschwerpunkte

Nach wie vor war für anlassunabhängige Prüfungen infolge der Belastung durch die Abarbeitung von Eingaben und Beratungsanfragen kaum Kapazität vorhanden: Die Personaldecke für die Bewältigung der Aufgaben ist eher knapp bemessen.

Die mit Abstand meisten Eingaben sind nach wie vor in den Fachgebieten Auskunfteien/Inkassounternehmen (im Wesentlichen infolge der Zuständigkeit für die SCHUFA Holding AG), Wohnen/Miete/Nachbarschaft (überwiegend wegen der in diesem Bereich anzutreffenden hohen Zahl von Videoüberwachungen) und elektronische Kommunikation und Internet zu verzeichnen. Aber auch in den Themenkomplexen Gesundheit/Pflege, Schulen/Hochschulen/Bildung; Soziales, Beschäftigtendatenschutz, Kreditwirt-

schaft/Spielbanken, Adresshandel/Werbung, Justiz/Polizei/Strafverfolgung, Kommunen und Verkehr sind konstant hohe Eingabezahlen zu verzeichnen.

Bei der Videoüberwachung war ein eklatanter Eingabenzuwachs aufgrund einer Sammeleingabe der Bürgerrechtsgruppe „*die*Datenschützer Rhein Main“ zu verzeichnen, die um eine Prüfung der Videoüberwachung an 378 einzeln aufgelisteten Stellen in Frankfurt am Main nachgesucht hat (s. a. Ziff. 5.2.1). In die Statistik sind davon bislang ca. 60 Fälle eingegangen, bei denen die Eigentümer bereits ermittelt wurden und hieraus ein Aktenfall entstanden ist.

Auch die vielfältigen Beratungsanfragen nehmen erhebliche Ressourcen meiner Dienststelle in Anspruch; hierzu zählt insbesondere auch die beratende Begleitung komplexer – oft mehrjähriger – Projektentwicklungen, z. B. im Bereich der technischen Infrastrukturen in Hessen.

Besonderen Stellenwert hat stets die Öffentlichkeitsarbeit einschließlich der Erstellung von Informationsmaterial wie z. B. „Aufgabe für App-Anbieter – Transparenz für Android App-Nutzer herstellen!“ (https://www.datenschutz.hessen.de/tf017.htm).

Hinsichtlich der Praxis von Ordnungswidrigkeitenverfahren sowie anderen Sanktions- und Meldungsregelungen nach dem BDSG (Zwangsgelder, Meldung von Datenpannen) wurde weiterhin Praxiserfahrung gesammelt. Hierzu finden regelmäßig Abstimmungen mit den anderen Aufsichtsbehörden – u. a. in der AG Sanktionen des Düsseldorfer Kreises – statt (zu den Ordnungswidrigkeitenverfahren s. a. Ziff. 5.1).

1.4.4
Statistik

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

Arbeitsstatistik des Hessischen Datenschutzbeauftragten

Dokumentierte Eingaben

Fachgebiet	Anzahl
Auskunfteien und Inkassounternehmen	319
Wohnen, Miete und Nachbarschaft	312
Elektronische Kommunikation, Internet	214
Gesundheit und Pflege	119
Schulen, Hochschulen, Bildung, Archive, Bibliotheken, Museen	115
Soziales	109
Beschäftigtendatenschutz	98
Polizei, Justiz, Strafvollzug und Gerichte	98
Kreditwirtschaft, Spielbanken, Lotto	97
Verkehr und Daseinsvorsorge	97
Werbung und Adresshandel	89
Kommunen	81
Versicherungen	39
Handel und Handwerk	34
Forschung, Planung und Statistik	28
Vereine und Verbände, Stiftungen, Parteien, Kammern	17
Rundfunk, Fernsehen, Presse	14
Sonstiges	37
Summe der dokumentierten Eingaben	**1.917**
Summe der dokumentierten Beratungsanfragen	**330**
davon Eingaben und Beratungen Videoüberwachung betreffend	396
Summe der telefonischen Eingaben und Beratungen	**4.896**
Gesamtsumme	**7.143**

Das Volumen stabilisiert sich auf konstant hohem Niveau. Beratungen waren in aller Regel deutlich aufwändiger als die Bearbeitung von Eingaben (z. B. Beratungen für komplexe Auftragsverhältnisse aus den unterschiedlichsten Fachgebieten, zu Binding Corporate Rules (BCR), grenzüber-

schreitendem Datenverkehr, zur datenschutzgerechten Ausgestaltung von Beförderungsbedingungen eines Verkehrsunternehmens, zu Cloud Computing, zur Ausgestaltung der Spielersperrdatei, zur datenschutzgerechten Gestaltung von Forschungsprojekten). Das Spektrum ist ebenso breit wie bei den Eingaben.

Im Berichtszeitraum beschäftigten mich auch wieder Ordnungswidrigkeitenverfahren. In 35 Fällen wurden neue Ordnungswidrigkeitenverfahren anhängig. In diesem Jahr habe ich 18 Verfahren eingestellt sowie zwei Verfahren mit einer Geldbuße abgeschlossen.

Betroffene sowie die zuständige Aufsichtsbehörde sind nach § 42a BDSG bei Verlust von personenbezogenen Daten und drohenden schwerwiegenden Beeinträchtigungen durch die verantwortliche datenverarbeitende Stelle unverzüglich zu informieren. In meinem 42. Tätigkeitsbericht habe ich die Meldepflicht bereits vorgestellt (vgl. Ziff. 4.1.2 Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten). Auch auf meiner Homepage www.datenschutz.hessen.de sind Informationen dazu abzurufen.

Die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG führte im Jahr 2014 zu 82 Meldungen bei mir. Davon waren 45 Meldungen tatsächlich solche, in denen eine Pflicht zur Information der Aufsichtsbehörde bestand.

2. Europa

2.1
Geplante Datenschutz-Grundverordnung und EU-Richtlinie für Polizei- und Justizbehörden

Das EU-Parlament hat noch vor der Neuwahl des Parlaments im Mai 2014 für das Datenschutzpaket gestimmt, während die Verhandlungen im Ministerrat weiterhin zäh verliefen. Das Datenschutzpaket umfasst eine Verordnung, die die Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich abdeckt, und eine Richtlinie, die die Verarbeitung personenbezogener Daten durch Polizei- und Justizbehörden betrifft. Der Beitrag zeigt die wesentlichen Entwicklungen für beide Bereiche im Berichtszeitraum auf.

2.1.1
EU-Datenschutz-Grundverordnungsentwurf

Im März folgte das Europaparlament mit dem Votum in 1. Lesung den Empfehlungen des Ausschusses für Bürgerliche Freiheit, Justiz und Inneres (Innenausschuss) (s. 42. Tätigkeitsbericht, Ziff. 3.1.1.1.1), die dieser im Oktober 2013 abgegeben hatte. Der Verordnungsentwurf wurde mit großer Mehrheit angenommen (s. a. Ziff. 1.1.3.1). Für das EU-Parlament gilt – anders als für den Deutschen Bundestag – nicht der Grundsatz der Diskontinuität. Dieser besagt, dass Gesetzesvorhaben, die innerhalb einer Legislaturperiode nicht verabschiedet werden, nach Ablauf dieser Periode verfallen. Die neu gewählten Abgeordneten des Europäischen Parlaments können deshalb entscheiden, ob sie auf dem Entwurf aufbauen wollen.

2.1.1.1
Position des EU-Parlaments

Die Vorschläge des Europäischen Parlaments enthalten u. a. folgende Elemente:

– Die Einwilligung soll weiterhin eine zentrale Rolle bei der Verarbeitung personenbezogener Daten spielen. Nur eine frei erteilte, ausdrückliche Einwilligung soll wirksam sein.
– Die Voraussetzungen für Datenübermittlungen in Drittstaaten sollen verschärft werden. Datenübermittlungen an ausländische Behörden sollen nur noch aufgrund von Rechtshilfeabkommen oder internationalen Vereinbarungen bei voller Transparenz gegenüber Datenschutzbehörden erlaubt sein. Damit würde der Datenschutz z. B. gegenüber ausländischen Geheimdiensten gestärkt.

– Die Betroffenen sollen ihre Rechte leichter geltend machen können, indem sie auf einfache und standardisierte Art über die Verarbeitung ihrer personenbezogenen Daten informiert werden.
– Die Prinzipien des Datenschutzes während der Entwicklung von Verarbeitungsverfahren (Datenschutz by design) und der datenschutzfreundlichen Voreinstellungen (Datenschutz by default) werden nach dem Vorschlag des Parlaments präzisiert und gestärkt.
– Der Parlamentsvorschlag knüpft bei Regelungen, die kleine und mittelständische Unternehmen entlasten sollen, an die Zahl der Datenverarbeitungen pro Jahr an. Die Ausnahmen sollen für Unternehmen gelten, die in einem Zeitraum von zwölf Monaten die Daten von bis zu 5000 Betroffenen bearbeiten.
– Als Maximalstrafe für Verstöße gegen die in der Verordnung festgelegten Regeln sind 100 Millionen EUR oder 5 Prozent des Jahresumsatzes eines Unternehmens vorgesehen (s. 42. Tätigkeitsbericht, Ziff. 3.1.1.1.1).

2.1.1.2
Verhandlungen im Ministerrat

Während sich das Parlament auf eine gemeinsame Position verständigen konnte und die Empfehlungen des Innenausschusses unverändert übernommen hat, verlief der Entscheidungsprozess im Ministerrat weiterhin schleppend. Unter dem griechischen Vorsitz im ersten Halbjahr 2014 wurde offensichtlich, dass über wesentliche Elemente nach wie vor gestritten wird. Bei der Ratstagung im März bekräftigten die Mitgliedstaaten, dass sichergestellt werden muss, dass Unionsvorschriften auf die Verarbeitung durch Verantwortliche, die nicht in der EU ansässig sind, angewendet werden, wenn sie personenbezogene Daten von in der Union ansässigen betroffenen Personen verarbeiten (Marktortprinzip).

Auf der Juni-Tagung des Rats verständigte man sich über einige Punkte hinsichtlich der Übermittlung personenbezogener Daten an Drittländer und an internationale Organisationen. Der Verordnungsentwurf der Kommission stellt in diesem Bereich eine Fortführung des Konzepts der Datenübermittlung auf der Grundlage von Angemessenheitsbeschlüssen dar. Dabei kann die Kommission feststellen, ob ein Drittland bzw. internationale Organisation einen angemessenen datenschutzrechtlichen Schutz bietet. Der Rat schlägt nun vor, dass der Europäische Datenschutzausschuss Stellungnahmen zu der Frage der Angemessenheit des Schutzniveaus abgibt. Ferner könnten, so der Rat, Datenübermittlungen an Drittländer gestattet sein, wenn der für die Verarbeitung Verantwortliche geeignete Garantien bietet.

Diese und weitere Vorschläge des griechischen Ratsvorsitzes haben im Rat breite Unterstützung durch die Mitgliedstaaten erfahren.

Im Oktober hat sich der Ministerrat auf weitere Punkte einigen können. Hierunter fallen unter anderem die Regelungen zu dem für die Datenverarbeitung Verantwortlichen, zur Auftragsdatenverarbeitung und zum betrieblichen Datenschutzbeauftragten. Ferner befürworten die Mitgliedstaaten einen risikobasierten Ansatz. Dieser zeichnet sich zum Beispiel dadurch aus, dass bestimmte Verpflichtungen (z. B. hinsichtlich der Dokumentationspflichten) nur für die höhere von zwei Risikogruppen („normal“ und „hoch“) gelten sollen. Die höhere Risikogruppe ist diejenige, bei der die Datenverarbeitung besonders hohe Gefahren für Persönlichkeitsrechte beinhalten kann. Anders als die Vorschläge von Kommission und Parlament sieht der Ministerrat keine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter vor, sondern nur eine Öffnungsklausel zugunsten der Mitgliedstaaten.

Die bisher getroffene Einigung im Rat stellt noch keine Grundlage dar, um in die Trilog-Verhandlungen mit Parlament und Kommission zu treten. Denn über einen großen Teil der Regelungen des Verordnungsentwurfs konnte im Ministerrat noch keine Einigung erzielt werden. Dies gilt insbesondere für die Rolle der Datenschutzaufsichtsbehörde im Nationalstaat. Hier stellt sich die Frage, ob, wie von der Kommission vorgeschlagen, eine einheitliche Anlaufstelle („One-Stop-Shop“) bürgerfreundlich ist. Nach dem Prinzip des One-Stop-Shop soll die Datenschutzbehörde am Sitz der Hauptniederlassung eines Unternehmens („Lead Authority“) EU-weit für die Aufsicht über alle Niederlassungen eines Unternehmens in der EU zuständig sein. Dabei werden folgende Fragen diskutiert:

– Aufteilung der Befugnisse zwischen „Lead Authority“ und nationaler Datenschutzbehörde
– Rechtsschutzmöglichkeiten der Bürgerinnen und Bürger
– Möglichkeit der Übertragung von Entscheidungsbefugnissen auf den Europäischen Datenschutzausschuss, in dem der Europäische Datenschutzbeauftragte und Vertreter der Mitgliedstaaten sitzen sollen

Die Diskussionen darüber, wie das Prinzip des One-Stop-Shop, gegebenenfalls unter Beteiligung des Europäischen Datenschutzausschusses, ausgestaltet werden kann, konnten im Berichtszeitraum nicht abgeschlossen werden.

2.1.1.3
Positionen und Vorschläge des Bundesinnenministeriums

Anfang des Jahres hat das Bundesinnenministerium einen eigenen Vorschlag zum „One-Stop-Shop“ veröffentlicht, da der Vorschlag der Kommission in der konkreten Ausgestaltung keine Unterstützung durch die Mitgliedstaaten erfahren hat. Der Vorschlag des Bundesinnenministeriums enthielt, vereinfacht dargestellt, zwei sich ergänzende Verfahren: Vorgesehen waren zum einen Rechtmäßigkeitsentscheidungen („Vorab-Genehmigungen“) zum geplanten Datenverarbeitungsvorgang im Interesse der Unternehmen und zum anderen Entscheidungen über die Rechtswidrigkeit einer Datenverarbeitung im Interesse der Bürger und der Aufsichtsbehörden. Dieser Vorschlag des Bundesministeriums wurde von den Datenschutzaufsichtsbehörden als kaum praktikabel kritisiert. Insbesondere die Rechtmäßigkeitsprüfung, die die Aufsichtsbehörden für Datenverarbeitungsvorgänge auf Antrag von Unternehmen ausführen sollen, stieß auf Ablehnung. Die Vorschläge des Bundesinnenministeriums fanden im EU-Ministerrat keine Mehrheit.

Mitte des Jahres stellte das Bundesinnenministerium in einem Schreiben die aus seiner Sicht wesentlichen Diskussionspunkte für die Datenschutzreform dar. Unter anderem fordert Deutschland eine Öffnungsklausel, die es Mitgliedstaaten ermöglicht, im öffentlichen Bereich strengere nationale Datenschutzbestimmungen zu erlassen. Der Ministerrat hat im Oktober einen Vorschlag vorgelegt, wonach es den Mitgliedstaaten erlaubt sein soll, nur solche Vorschriften betreffend das öffentliche Datenschutzrecht zu erhalten oder neu zu schaffen, die die Vorgaben der vorgeschlagenen Grundverordnung präzisieren. Deutschland kritisierte, dass diese Öffnungsklausel nicht ausreichend sei. Im Berichtszeitraum konnte insofern keine Einigung im Ministerrat erreicht werden. Weitere Kernfrage ist aus deutscher Sicht die Datenübermittlung in Drittstaaten.

Die italienische Ratspräsidentschaft strebt bis Dezember d. J. eine Einigung zu diesen und weiteren Fragen des Verordnungsvorschlags an.

2.1.1.4
Zeitlicher Rahmen

Aufgrund des immer noch fehlenden Konsenses im Ministerrat ist mit einem baldigen Beginn der Trilog-Verhandlungen nicht zu rechnen. Ob über die vorgenannten Punkte und über die zahlreichen offenen Fragen im Ministerrat zeitnah eine Einigung zu erzielen ist, ist im Berichtszeitraum noch nicht absehbar. Damit bleibt ungewiss, ob die Reform, wie von der Kommission

gewünscht, im Jahr 2015 verabschiedet werden kann. Der Bundesinnenminister äußerte sich allerdings jüngst dahingehend, dass der europäische Datenschutz 2015 geregelt werden solle (Frankfurter Allgemeine Sonntagszeitung vom 21. Sept. 2014, S. 21).

2.1.2
EU-Richtlinie für Polizei- und Justizbehörden

Nachdem sich das Parlament auch hinsichtlich der Richtlinie für die Datenverarbeitung durch Polizei- und Justizbehörden auf einen gemeinsamen Standpunkt – zeitgleich zur Einigung über die Datenschutz-Grundverordnung – einigen konnte, gab es im Ministerrat kaum Fortschritte. Im Berichtszeitraum fanden mehrere Sitzungen der zuständigen Ratsarbeitsgruppe DAPIX (Data Protection and Information Exchange Working Group) statt, in denen die Richtlinie behandelt wurde. Dabei wurde eine Neufassung zahlreicher Vorschriften erstellt.

Neben Deutschland hegen viele andere Mitgliedstaaten grundsätzliche Bedenken. Zentrale Fragen, etwa zum Anwendungsbereich der Richtlinie, dem Verhältnis der Richtlinie zur Datenschutz-Grundverordnung und den Rechten der Betroffenen, waren im Berichtszeitraum noch offen. Da eine Evaluierung des bislang in diesem Bereich geltenden Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der politischen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (EU-Ratsdokument 9260/08), durch die Kommission noch aussteht, erheben verschiedene Mitgliedstaaten die Frage, ob der Richtlinienvorschlag tatsächlich eine Verbesserung gegenüber dem Status quo bedeutet.

Die Kommission hält nach wie vor an der „Paketlösung“ fest, das heißt, dass Grundverordnung und Richtlinie gemeinsam verabschiedet werden sollen. Neue Berichterstatterin des Parlaments für die Richtlinie ist die Vertreterin Estlands Frau Marju Lauristin.

2.2
„Smart Borders“ – Intelligente Grenzen an den Außengrenzen der EU

Das Reformpaket „Intelligente Grenzen“ habe ich in den Grundzügen bereits im 42. Tätigkeitsbericht dargestellt. Im Berichtszeitraum ist dieses gesetzgeberische Vorhaben weiter vorangeschritten. Vieles deutet darauf hin, dass nur noch das „Wie“ der Umsetzung des Reformvorhabens zu klären ist, nicht mehr das „Ob“.

2.2.1
Die Entwicklung des Reformprojekts im Berichtszeitraum

Seit Vorstellung der Kommissionsvorschläge im vergangenen Jahr (s. 42. Tätigkeitsbericht, Ziff. 3.1.5) ist das Vorhaben rasant vorangekommen. CDU und SPD verständigten sich in ihrem Koalitionsvertrag darauf, dass Einreiseerleichterungen nach Europa „ein Ein- und Ausreiseregister im europäischen Verbund“ voraussetzen. Wie die meisten anderen Mitgliedstaaten ist damit auch Deutschland Befürworter des „Smart Borders“-Pakets, das der Eindämmung der irregulären Migration dienen soll. Das Maßnahmenpaket würde nach dem gegenwärtigen Stand etwa 1,35 Milliarden EUR kosten und von der neuen Agentur für das Betriebsmanagement von IT-Großsystemen (EU-LISA) verwaltet. Die in Tallinn, Estland, ansässige Agentur ist seit Dezember 2012 zuständig für die Datenbanken SIS (Schengener Informationssystem), EURODAC (Europäisches Fingerabdrucksystem) und VIS (Visa-Informationssystem).

Das Einreise- und Ausreisesystem (EES) ist neben dem Registrierungsprogramm für Vielreisende (RTP) die Hauptkomponente des Maßnahmenpakets. Nach dem Vorschlag der Kommission werden für das EES zunächst alphanumerische Daten gespeichert (u. a. Name, Nummer des Reisedokuments, Datum der Ein- und Ausreise) und, nach einer Übergangszeit von drei Jahren, auch biometrische Daten, wobei die Speicherung von zehn Fingerabdrücken gegenwärtig bevorzugt wird.

Im November 2013 gab die Kommission eine Studie einschließlich eines Testlaufs der nötigen IT-Systeme („proof of concept“, Machbarkeitsnachweis) in Auftrag. Die Studie, die im Oktober veröffentlicht wurde, umfasst zwanzig Themenbereiche unter den Überschriften Biometrie, Auswirkungen auf den Grenzübertrittsprozess, Daten, Architektur und Sonstiges. Anhand der Studie sollen bis Dezember die Kernelemente des Pilotprojekts festgelegt werden, das im Januar 2015 beginnen und bis zum Jahresende laufen soll. Im Berichtszeitraum wurde das von der Kommission vorgeschlagene Maßnahmenpaket weder im EU-Parlament noch im Ministerrat diskutiert bzw. verabschiedet. Die Kommission erklärte, die Durchführung des Machbarkeitsnachweises dürfe nicht dazu führen, dass sich Verhandlungen zu dem Thema verzögerten. Eine Einigung zwischen Parlament und Rat könne so möglicherweise bereits 2016 erfolgen.

2.2.2

Datenschutzrechtliche Bedenken vor dem Hintergrund des Urteils des EuGH zur Vorratsdatenspeicherung

Bereits im vergangenen Jahr zeichnete sich ab, dass neben der Bekämpfung der irregulären Migration durch so genannte „Overstayer", das heißt Drittstaatsangehörige, die ihre zulässige Aufenthaltsdauer überziehen, die Gefahrenabwehr und Strafverfolgung weitere Ziele des Reformprojekts sein sollen. Dies wird von der BTLE-Arbeitsgruppe, die sich auch dieses Jahr wieder mit dem Projekt befasst hat, kritisch gesehen. In der Arbeitsgruppe BTLE (Border, Travel, Law Enforcement), einer Unterarbeitsgruppe der europäischen Art. 29-Datenschutzgruppe, arbeitet meine Mitarbeiterin als Vertreterin der Landesdatenschutzbehörden mit. Der Verordnungsentwurf der Kommission sieht die Prüfung eines Zugangs der Strafverfolgungsbehörden zwei Jahre nach Inbetriebnahme des EES vor. Für diesen Zweck sollen die gespeicherten Daten polizeilich genutzt werden können. Es sei unstreitig, so die Bundesregierung, „dass bessere statistische Erkenntnisse zur Zahl der Overstayer allein die Einführung eines EES nicht rechtfertigen können." (BTDrucks. 18/455). Eine Reihe von Mitgliedstaaten habe laut Bundesregierung „Zweifel am Kosten-Nutzen-Verhältnis", „wenn das EES nicht auch zur Verhütung und Verfolgung terroristischer und sonstiger schwerwiegender Straftaten genutzt werden könne" (ebenda). Ferner habe sich die Mehrheit der Mitgliedstaaten dafür ausgesprochen, von Anfang an einen Zugang zum EES zu Zwecken der Verhütung und Verfolgung terroristischer und sonstiger schwerer Straftaten vorzusehen.

Wird über einen Zugriff der Strafverfolgungsbehörden auf die neue Datenbank nachgedacht, so ist in diesem Zusammenhang das Urteil des Europäischen Gerichtshofs (EuGH) vom 8. April 2014 zur Vorratsdatenspeicherung zu berücksichtigen (Verbundene Rechtssachen C-293/12 und C-594/12). Der EuGH hat entschieden, dass die Richtlinie zur Vorratsdatenspeicherung gegen europäisches Recht verstößt und ungültig ist. Die Regelung „beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt", so die Richter. Werden personenbezogene Daten in einer neuen Datenbank gespeichert und soll den Strafverfolgungsbehörden Zugriff gewährt werden, so sind die in dem Urteil genannten Anforderungen, insbesondere an die Erforderlichkeit des Zugriffs und die notwendigen Sicherheitsmaßnahmen zum Schutz der Daten, zu berücksichtigen. Es bedarf unter anderem objektiver Kriterien, nach denen bestimmt werden kann, welche Behörden zu welchem Zweck Zugriff auf welche Daten ha-

ben. Auch die Dauer der Datenspeicherung muss klar und nachvollziehbar geregelt sein.

Diese Fragen werden in der Arbeitsgruppe BTLE weiterhin unter meiner Beteiligung intensiv diskutiert.

2.2.3
Zeitlicher Rahmen

Bis Mitte 2016 wollen die Mitgliedstaaten die Verhandlungen über das Maßnahmenpaket weitgehend abgeschlossen haben. Bis Januar 2019 soll das System anschließend entwickelt und bis Mitte 2020 errichtet werden. Start von „Smart Borders“ wäre nach gegenwärtigem Zeitplan etwa in der Mitte des Jahres 2020, also in etwa sechs Jahren. Ob dieser Zeitplan angesichts der Erfahrungen mit der Datenbank SIS II (s. 42. Tätigkeitsbericht, Ziff. 3.1.5) eingehalten werden kann, erscheint fraglich. SIS II sollte ursprünglich 2007 in Betrieb gehen, die tatsächliche Inbetriebnahme erfolgte aus unterschiedlichen Gründen erst im April 2013.

2.3
EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Im August ist die Verordnung über elektronische Identifizierung und Vertrauensdienste im Amtsblatt veröffentlicht worden. Die Folgen für Deutschland sind noch nicht absehbar.

Bereits im 41. Tätigkeitsbericht (Ziff. 2.1.1) und 42. Tätigkeitsbericht (Ziff. 3.1.2) habe ich mich kritisch mit der geplanten Verordnung auseinandergesetzt. Die Verordnung trat nunmehr im September 2014 in Kraft. Personen und Unternehmen sollen mit ihrer eigenen elektronischen Identifizierung (eID) öffentliche Dienste in anderen EU-Mitgliedstaaten benutzen können, wenn für die Dienste eine eID verlangt wird. Die Mitgliedstaaten werden hierzu verpflichtet, die Systeme der eID anderer Mitgliedstaaten unter bestimmten Voraussetzungen anzuerkennen. Dabei müssen nur Anwendungen, die das Sicherheitsniveau „substantiell“ oder „hoch“ verlangen, notifizierte eIDs akzeptieren. Eine Pflicht zur Anerkennung besteht ab dem 18. September 2018.

Mitgliedstaaten können zukünftig zudem nationale Systeme zur eID bei der EU-Kommission anmelden, überprüfen und gegebenenfalls als „sicher“ einstufen lassen. Die Verordnung bezieht sich ferner auf elektronische Signaturen, Zeitstempel und Siegel. Eingeschlossen sind auch Verfahren zur

Webseiten-Authentifizierung. Die Vertrauensdienste sollen grenzüberschreitend in ganz Europa funktionieren und den gleichen Rechtsstatus haben wie papiergestützte Verfahren. In vielen Fällen bedarf es noch eines Durchführungsrechtsaktes zur Präzisierung der in der Verordnung getroffenen Regelungen.

Die Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen wird mit Wirkung vom 1. Juli 2016 aufgehoben, ab diesem Zeitpunkt gilt – sofern nicht ein anderer Geltungszeitpunkt in der Verordnung festgelegt wird – ein Großteil der neuen Regelungen der Verordnung. Notifizierungen werden voraussichtlich ab September 2015 möglich sein, sobald die Durchführungsrechtsakte zu den Sicherheitsniveaus und Interoperabilitätsrahmen anwendbar ist. Ob die Interoperabilität in der Praxis umsetzbar sein wird, bleibt abzuwarten. Im Zweifel können die nationalen Regelungen bis 2019 etwaige Regelungslücken füllen, wenn die Durchführungsrechtsakte nicht rechtzeitig verabschiedet wird.

Welche Folgen die Verordnung für die qualifizierte elektronische Signatur in Deutschland haben wird, wenn europaweit nur fortgeschrittene Signaturen – mit einem geringeren Sicherheitsniveau – gelten, muss sich noch zeigen. Auf jeden Fall werden zukünftig auch andere Signaturen aus europäischen Mitgliedstaaten in Deutschland anerkannt werden müssen. Auch die Tatsache, dass Verschlüsselungszertifikate für jede E-Mail-Adresse mit einem Escrow-Verfahren beim TSP gespeichert werden und eine Ende-zu-Ende-Verschlüsselung aufgehoben werden kann, ist u. a. von den Datenschutzbeauftragten kritisiert worden.

2.4
Koordinierte Kontrollgruppe für das SIS II

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrung der Interessen der Landesdatenschutzbeauftragten in der Koordinierten Kontrollgruppe für das SIS II übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an zwei Sitzungen in Brüssel teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2014 dar.

Mit Inbetriebnahme des SIS II im März vergangenen Jahres ist die Kontrolle von der Gemeinsamen Kontrollinstanz auf den Europäischen Datenschutzbeauftragten (EDPS) übergegangen. Dieser trifft sich mindestens zweimal jährlich mit den nationalen Kontrollinstanzen als sog. Koordinierte Kontrollgruppe für das SIS II (CSG SIS II Coordinated Supervision Group). Wichtig aus deutscher Sicht war die Behandlung des Problems der Aus-

schreibungen von gestohlenen oder sonst abhandengekommenen Kraftfahrzeugen (s. 42. Tätigkeitsbericht, Ziff. 3.1.3.3), aber auch die Aktualisierung von Dokumenten und Stellungnahmen anhand des neuen Rechtsrahmens.

2.4.1
Ausschreibungen von gestohlenen Kraftfahrzeugen im SIS II

Im 42. Tätigkeitsbericht hatte ich von Problemen im Zusammenhang mit der unterbliebenen Löschung von im SIS II ausgeschriebenen Kraftfahrzeugen berichtet. Die Kontrollgruppe hat das Thema in der Sitzung im Mai d. J. ausführlich besprochen.

Meine Mitarbeiterin stellte dort die praktischen Probleme und rechtlichen Aspekte dar. Zu den praktischen Problemen des Erwerbers eines im SIS II ausgeschriebenen Kraftfahrzeuges zählen die eingeschränkten Möglichkeiten beim Wiederverkauf und bei Reisen mit dem Fahrzeug innerhalb des Schengen-Raums. Da zahlreiche Fälle dieser Art bei dem deutschen SIRENE-Büro (**S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntity) als zuständiger Kontaktstelle für SIS-Anfragen auflaufen, versuchte die Kontrollgruppe, einen gemeinsamen Standpunkt zum Umgang mit streitigen Löschungsersuchen zu finden.

Meine Mitarbeiterin vertrat dabei den Standpunkt, dass mit dem Auffinden des Kraftfahrzeugs der Zweck der SIS-Ausschreibung gemäß Artikel 38 des Beschlusses 2007/533/JI erfüllt sei.

Artikel 38 SIS II Beschluss 2007/533/JI

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

(2) Es werden folgende Kategorien von leicht identifizierbaren Sachen einbezogen:
a) Kraftfahrzeuge mit einem Hubraum von mehr als 50 ccm, Wasserfahrzeuge und Luftfahrzeuge;

...

Sobald der ausschreibende Mitgliedstaat über das Auffinden und über die Möglichkeit, ein Rechtshilfeersuchen zu stellen, unterrichtet worden sei, sei die Löschung der betreffenden Daten angezeigt. Delegationen einzelner Mitgliedstaaten äußerten Verständnis für den deutschen Standpunkt, wiesen aber darauf hin, dass die betreffenden Fahrzeuge teilweise Gegenstand eines justiziellen oder gerichtlichen Verfahrens seien und eine Datenlöschung bis zum Abschluss dieses Verfahrens nicht statthaft sei.

Die Mitgliedstaaten waren sich zu Abschluss der Diskussion zum einen darüber einig, dass eine dauerhafte Ausschreibung nicht mit dem Zweck der Datenerhebung vereinbar sei und es eine Höchstdauer für die Ausschreibung geben müsse. Es sei nicht hinnehmbar, dass sich der ausschreibende Mitgliedstaat auf die Mitteilung eines anderen Mitgliedstaats, man habe das Kraftfahrzeug gefunden und es könne ein Rechtshilfeersuchen gestellt werden, nicht äußert. Zum anderen bestand Einigkeit darüber, dass die Kontrollgruppe ausschließlich für die datenschutzrechtlichen Aspekte der betreffenden Fallkonstellationen zuständig sei.

Unterstützung erhielt die deutsche Auslegung der betreffenden Rechtsvorschriften durch die in der Sitzung anwesende Vertreterin der Europäischen Kommission. Der Ausschuss für das Schengener Informationssystem der zweiten Generation und das Visa-Informationssystem (SIS-VIS-Ausschuss), der unter dem Vorsitz der Kommission zusammentritt, vertritt gleichfalls die Auffassung, dass Justiz- oder Gerichtsverfahren das Aufrechterhalten einer Ausschreibung über mehrere Jahre nicht rechtfertigen können. Grundsätzlich sei davon auszugehen, dass mit dem Auffinden von gesuchten Objekten und der entsprechenden Mitteilung an den ausschreibenden Mitgliedstaat der Zweck der Ausschreibung erfüllt sei.

In der Oktober-Sitzung verständigte sich die Kontrollgruppe darauf, eine entsprechende datenschutzrechtliche Stellungnahme zur Handhabung der betreffenden Fälle zu erstellen.

Die Eingabe eines betroffenen Petenten aus Hessen, die unter anderem Anlass für die Diskussion in der Kontrollgruppe war, hat sich im Frühjahr d. J. zufriedenstellend erledigt. Die entsprechenden Daten wurden aus der SIS-Datenbank nach vier Jahren und zahlreichen Gesprächen zwischen den beteiligten Stellen aus beiden Mitgliedstaaten gelöscht. Aufgrund der intensiven Auseinandersetzung mit diesem Thema auf europäischer Ebene besteht Hoffnung, dass vergleichbare Fälle zukünftig zügig behandelt werden können.

2.4.2
Leitfaden zum Auskunftsrecht in allen Schengen-Staaten

Die Kontrollgruppe hat den bereits im Jahr 2009 erstellten Leitfaden (38. Tätigkeitsbericht, Ziff. 2.2.4) überarbeitet und den neuen Rechtsgrundlagen angepasst. Nach wie vor besteht im Zusammenhang mit dem Schengener Informationssystem die Besonderheit, dass jede Person in jedem Schengen-Staat Auskunft bzw. Berichtigung oder Löschung über die zu ihr gespeicherten Daten verlangen kann, unabhängig davon, welcher Staat die Ausschreibung veranlasst hat.

Artikel 41 der SIS II-Verordnung (EG) Nr. 1987/2006

1. *Das Recht jeder Person, über die gemäß dieser Verordnung zu ihrer Person im SIS II gespeicherten Daten Auskunft zu erhalten, richtet sich nach dem Recht des Mitgliedstaats, in dessen Hoheitsgebiet das Auskunftsrecht beansprucht wird.*
2. *Soweit das nationale Recht dies vorsieht, entscheidet die nationale Kontrollinstanz, ob und in welcher Weise Auskunft erteilt wird.*
3. *Ein Mitgliedstaat, der die Ausschreibung nicht vorgenommen hat, darf Auskunft zu diesen Daten nur erteilen, wenn er vorher dem ausschreibenden Mitgliedstaat Gelegenheit zur Stellungnahme gegeben hat. Dies erfolgt im Wege des Austauschs von Zusatzinformationen.*
4. *Die Auskunftserteilung an die betroffene Person unterbleibt, wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit einer Ausschreibung oder zum Schutz der Rechte und Freiheiten Dritter unerlässlich ist.*
5. *Jeder hat das Recht, auf seine Person bezogene sachlich unrichtige Daten berichtigen oder unrechtmäßig gespeicherte Daten löschen zu lassen.*
6. *Der Betroffene wird so schnell wie möglich informiert, spätestens jedoch 60 Tage nach Stellung seines Antrags auf Auskunft oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen.*
7. *Der Betroffene wird so schnell wie möglich, spätestens jedoch drei Monate nach Stellung seines Antrags auf Berichtigung oder Löschung, oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen, davon in Kenntnis gesetzt, welche Maßnahmen zur Wahrung seines Rechts auf Berichtigung oder Löschung getroffen wurden.*

Artikel 58 SIS II Beschluss 2007/533/JI

(1) Das Recht jeder Person, über die gemäß diesem Beschluss zu ihrer Person in das SIS II gespeicherten Daten Auskunft zu erhalten, richtet sich nach dem Recht des Mitgliedstaats, in dessen Hoheitsgebiet das Auskunftsrecht beansprucht wird.

(2) Soweit das nationale Recht dies vorsieht, entscheidet die nationale Kontrollinstanz, ob und in welcher Weise Auskunft erteilt wird.

(3) Ein Mitgliedstaat, der die Ausschreibung nicht vorgenommen hat, darf Auskunft zu diesen Daten nur erteilen, wenn er vorher dem ausschreibenden Mitgliedstaat Gelegenheit zur Stellungnahme gegeben hat. Dies erfolgt im Wege des Austauschs von Zusatzinformationen.

(4) Die Auskunftserteilung an den Betroffenen unterbleibt, wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit einer Ausschreibung oder zum Schutz der Rechte und Freiheiten Dritter unerlässlich ist.

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

(6) Der Betroffene wird so schnell wie möglich informiert, spätestens jedoch 60 Tage nach Stellung seines Antrags auf Auskunft oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen.

(7) Der Betroffene wird so schnell wie möglich, spätestens jedoch drei Monate nach Stellung seines Antrags auf Berichtigung oder Löschung, oder früher, wenn die nationalen Rechtsvorschriften dies vorsehen, davon in Kenntnis gesetzt, welche Maßnahmen zur Wahrung seines Rechts auf Berichtigung oder Löschung getroffen wurden.

Inhaltlich neu sind die in Art. 41 Nrn. 6 und 7 SIS II-Verordnung und Art. 58 Nrn. 6 und 7 SIS II-Beschluss enthaltenen Fristen für die Antwort an den Betroffenen bzw. für dessen Information über die getroffenen Maßnahmen.

Da sich die Bürger an alle Aufsichtsbehörden der Schengen-Staaten wenden können und dann nationales Recht Anwendung findet, hat die Kontrollgruppe die wichtigsten Verfahrensschritte zur Geltendmachung der Rechte in den jeweiligen Schengen-Staaten sowie die aktuellen Adressen der zuständigen Behörden zusammengestellt. Des Weiteren wurden Formbriefe für die Bitte um Auskunft, Löschung oder Berichtigung entwickelt.

2.4.3
Bericht über die tatsächliche Ausübung der Rechte der Betroffenen

Die Kontrollgruppe hat ein schon vor längerer Zeit begonnenes Projekt zu Ende geführt. Die Ergebnisse der in allen 28 Schengen-Staaten bearbeiteten Fragebögen zu Einzelheiten der Geltendmachung der Auskunfts-, Berichtigungs- und Löschungsrechte von betroffenen Bürgern wurden in dem Bericht zusammengefasst.

Angesichts der derzeit im SIS II befindlichen über 45 Millionen Ausschreibungen zu Personen und Sachen erscheinen die jährlich etwa 4000 bis 5000 schengenweiten Auskunfts-, Berichtigungs- und Löschungsbegehren sehr gering. Einer der maßgeblichen Gründe hierfür liegt darin, dass viele Bürger, insbesondere Drittstaatsangehörige, keine Kenntnis von den ihnen zustehenden Rechten haben. Hier tut Aufklärung not, insbesondere die Zusammenarbeit mit Nichtregierungsorganisationen (NGOs), die mit Immigranten zusammenarbeiten. Kritisch sieht der Bericht die in mehreren Schengen-Staaten geübte Praxis, Standardauskünfte zu geben. Zwar kann das Auskunftsrecht beschränkt werden, insbesondere bei laufenden Ermittlungen, es muss aber jedes Mal eine Einzelfallentscheidung erfolgen.

2.4.4
Abgleich von Meldevordrucken in Hotels mit dem SIS II

Die Kontrollgruppe hat die im Jahr 2011 verfasste Stellungnahme zu Problemen des Abgleichs von den in Hotels auszufüllenden Meldevordrucken mit dem SIS II (39. Tätigkeitsbericht, Ziff. 2.3.4) den neuen Rechtsgrundlagen für das SIS II angepasst.

Danach können die von den ausländischen Gästen ausgefüllten Meldevordrucke in Beherbergungsstätten für die Polizeibehörden bereitgehalten oder diesen übermittelt werden, wenn dies u. a. zur Gefahrenabwehr oder

zur Strafverfolgung erforderlich ist. Ein regelmäßiger Abgleich mit dem SIS II ohne besondere Anhaltspunkte für einen bestimmten Verdacht ist deshalb nach wie vor nicht zulässig. Zwar können im nationalen Recht gewisse Abweichungen hiervon vorgenommen werden, ein 100%iger Abgleich mit dem SIS II ist aber – wie im Rahmen der alten Rechtslage – nicht zulässig.

Die deutsche Rechtslage entspricht diesen Vorgaben. Derzeit gelten noch:

§ 16 Abs. 3 MRRG

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

Die entsprechende Vorschrift im Hessischen Meldegesetz lautet:

§ 27 Abs. 3 HMG

Die Meldescheine sind von den Verantwortlichen in den Beherbergungsstätten für die Polizeibehörden und -dienststellen, die Staatsanwaltschaften und die Meldebehörden zur Einsichtnahme bereitzuhalten. Auf Verlangen sind sie den Polizeibehörden und -dienststellen und den Staatsanwaltschaften zur Mitnahme auf die Dienststelle auszuhändigen und erforderlichenfalls im Einzelfall zum Verbleib zu überlassen. Sie sind ein Jahr aufzubewahren, vor unbefugter Einsichtnahme zu sichern und innerhalb eines weiteren halben Jahres zu vernichten. Meldescheine von Stammgästen (§ 26 Abs. 2 Satz 7) dürfen bis zu zwei Jahre aufbewahrt werden.

Die dem Bund nach der Föderalismusreform I im Jahr 2006 zugewiesene ausschließliche Gesetzgebungskompetenz für das Meldewesen gemäß Art. 73 Abs. 1 Nr. 3 GG wurde durch das Bundesmeldegesetz (BMG) wahrgenommen, das am 1. November 2015 in Kraft treten wird.

Die entsprechende Vorschrift lautet:

§ 30 Abs. 4 BMG

Die Leiter der Beherbergungsstätten oder der Einrichtungen nach § 29 Absatz 4 haben die ausgefüllten Meldescheine vom Tag der Anreise der beherbergten Person an ein Jahr aufzubewahren und innerhalb von drei Monaten der Aufbewahrungsfrist zu vernichten. Die Meldescheine sind den nach Landesrecht bestimmten Behörden und den in § 34 Absatz 4 Satz 1 Nummer 1 bis 5 und 9 bis 11 genannten Behörden zur Erfüllung ihrer Aufgaben auf Verlangen zur Einsichtnahme vorzulegen. Die Meldescheine sind so aufzubewahren, dass keine unbefugte Person sie einsehen kann.

Auch diese Vorschrift entspricht den Vorgaben der SIS II-Rechtsgrundlagen.

2.5
Gemeinsame Kontrollinstanz für Europol

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrung der Interessen der Landesdatenschutzbeauftragten in der Gemeinsamen Kontrollinstanz für Europol übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an vier Sitzungen in Brüssel sowie an Treffen von Arbeitsgruppen teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2014 dar.

2.5.1
Neue Rechtsgrundlage für Europol

Die geplante neue Rechtsgrundlage für Europol wurde von mir bereits im 41. Tätigkeitsbericht (Ziff. 3.1.2) und im 42. Tätigkeitsbericht (Ziff. 3.1.4.3) behandelt.

Der Kommissionsentwurf (COM(2013) 173 endg.) ist im Berichtszeitraum überarbeitet worden.

Der Rat hat sich auf seiner Tagung Anfang Juni dieses Jahres auf eine allgemeine Ausrichtung zu diesem Vorschlag geeinigt. Diese Ausrichtung ist Grundlage für Verhandlungen mit dem Europäischen Parlament über die endgültige Fassung der Verordnung (Rat der Europäischen Union 28. Mai 2014, 10033/14).

Die Gemeinsame Kontrollinstanz (GKI) hat die Änderungen eingehend diskutiert und sich in einer dritten Stellungnahme dazu geäußert. Die wichtigsten Punkte sind folgende:

– Die restriktive Regelung für die Verarbeitung der Daten von Opfern von Straftaten, Zeugen, aber auch von Minderjährigen, wie sie im Vorentwurf vorgesehen war, soll beibehalten werden.
– Auch eine aus datenschutzrechtlicher Sicht festzustellende Schlechterstellung des Betroffenen bei der Geltendmachung seines Auskunftsrechts gegenüber Europol soll vermieden werden. Europol hat zwar den im Einzelfall betroffenen Mitgliedstaat vor der Auskunftserteilung zu konsultieren. Europol soll aber – wie es im Vorentwurf vorgesehen war – seine eigene Abwägung der für oder gegen eine Auskunftserteilung sprechenden Gründe vornehmen können, ohne dabei an die Auffassung des Mitgliedstaates gebunden zu sein.
– Ein weiterer wichtiger Vorschlag betrifft die Zusammenarbeit zwischen dem Europäischen Datenschutzbeauftragten und den nationalen Datenschutzaufsichtsbehörden. Die GKI hatte in den vorausgehenden Stel-

lungnahmen betont, dass die nationalen Aufsichtsbehörden bei der Kontrolle von Europol einen wichtigen Beitrag leisten müssten, da der größte Teil der von Europol verarbeiteten Daten von den Mitgliedstaaten stammt (siehe 42. Tätigkeitsbericht, Ziff. 3.1.4.3). Der Änderungsentwurf berücksichtigt diese Überlegungen. Vorgesehen ist nunmehr, dass ein Beirat für die Zusammenarbeit (Cooperation Board) geschaffen wird, der aus dem Europäischen Datenschutzbeauftragten und den nationalen Kontrollbehörden besteht. Damit wird die schon im Vorentwurf vorgesehene Zusammenarbeit institutionalisiert. Durch die Festlegung einer Reihe von wichtigen Aufgaben des Beirats wird die Rolle der nationalen Kontrollbehörden im Verhältnis zum Europäischen Datenschutzbeauftragten gestärkt.

Auf Wunsch der deutschen Delegation in der GKI enthält die Stellungnahme einen Änderungsvorschlag zur Zusammensetzung des Beirats. Dieser soll nicht – wie vorgesehen – aus einem, sondern aus bis zu zwei Vertretern der jeweiligen nationalen Kontrollbehörde bestehen. Damit würde sichergestellt, dass weiterhin sowohl ein Vertreter der Bundesbeauftragten für Datenschutz und Informationsfreiheit als auch ein Vertreter der Landesdatenschutzbeauftragten im Beirat vertreten sein können. Aus deutscher Sicht erscheint es wichtig, dass die Interessen der Bundesländer, die für einen großen Teil der Datenverarbeitung gerade im Polizeibereich zuständig sind, eigenständig repräsentiert sind.

2.5.2
Europol als Dienstleister (Serviceprovider) für die Mitgliedstaaten

Im 42. Tätigkeitsbericht (Ziff. 3.1.4.1) hatte ich über Bestrebungen von Europol berichtet, als bloßer Serviceprovider für die Mitgliedstaaten zu fungieren, und als Beispiel dafür die geplante Ausweitung der Kommunikation im Rahmen des bestehenden Informationsaustauschnetzes [**S**ecure **I**nformation **E**xchange **N**etwork **A**pplication (SIENA)] genannt. Die GKI hatte in einer Stellungnahme klargestellt, dass es für bestimmte Übermittlungen keine gesetzliche Grundlage im Europol-Beschluss (Beschluss des Rates zur Errichtung des Europäischen Polizeiamtes (Europol) vom 6. April 2009, ABl. L121/37) gibt.

In dem überarbeiteten Entwurf für eine Europol-Verordnung (Stand 28. Mai 2014) findet sich nunmehr in Erwägungsgrund 20 die Zielsetzung, dass Europol in umfassender Weise als Serviceprovider agieren und das Netzwerk SIENA für den Datenaustausch nicht nur zwischen Mitgliedstaaten, sondern auch Drittstaaten und internationalen Organisationen bereitstellen soll.

2.5.3
Zusammenarbeit von Europol mit den zentralen Meldestellen in den Mitgliedstaaten zur Verhinderung der Geldwäsche

Die nach der Geldwäscherichtlinie (2005/60/EG; ABl. L 309 vom 25. November 2005) in den Mitgliedstaaten errichteten zentralen Meldestellen (Financial Intelligence Units, FIU) kommunizieren über ein eigenes Netzwerk, das FIU.NET. Nach Plänen von Europol soll dieses Netzwerk in das o. g. Informationsaustauschnetz SIENA von Europol integriert werden.

Die GKI hat in einer Stellungnahme dargelegt, dass der geltende Europol-Beschluss eine derartige Zusammenarbeit nicht zulässt. Sie ist der Auffassung, dass die in der Geldwäscherichtlinie genannten Behörden keine „zuständigen Behörden" im Sinne des Europol-Beschlusses sind. Auch dieses Problem könnte durch den europäischen Gesetzgeber gelöst werden, da in dem überarbeiteten Entwurf für eine Europol-Verordnung eine Bestimmung aufgenommen wurde, die die Mitgliedstaaten dazu verpflichtet, die Voraussetzungen für eine Zusammenarbeit zwischen den nationalen Meldestellen und Europol zu schaffen.

2.6
Google-Urteil des EuGH

Dem Europäischen Gerichtshof zufolge kann eine Person, wenn bei einer anhand ihres Namens durchgeführten Suche in der Trefferliste der Suchmaschine ein Link zu einer Webseite mit Informationen über sie angezeigt wird, unter bestimmten Voraussetzungen vom Suchmaschinenbetreiber verlangen, den Link aus der Trefferliste zu entfernen. Das Urteil stellt die Aufsichtsbehörden vor eine Reihe von Auslegungsfragen.

2.6.1
Sachverhalt

Dem Urteil lag ein Sachverhalt aus Spanien zugrunde. Die katalanische Tageszeitung La Vanguardia hat ein Archiv seiner alten Druckausgaben online gestellt. Auf einer Zeitungsseite vom 19. Januar 1998 und einer vom 9. März 1998 wird u. a. die Zwangsversteigerung einer Immobilie des spanischen Staatsbürgers Mario Costeja González angekündigt. Herr Gonzáles hatte seine Schulden bei der Sozialversicherung nicht bezahlt, die deshalb die Zwangsversteigerung betrieb. Bei Eingabe des Vornamens und Nachnamens in die Suchmaschine Google Search erschienen in der Ergebnisliste Links zu den beiden Seiten. Im November 2009 wandte sich Herr Gonzáles

an den Verleger der Tageszeitung und beanstandete, dass bei Eingabe seines Namens in die Suchmaschine Google Search ein Link auf die Seiten mit der Bekanntmachung der Immobilienversteigerung erscheine. Die Pfändung wegen der Schulden bei der Sozialversicherung sei seit Jahren erledigt und derzeit ohne Bedeutung. Die Zeitung verweigerte eine Löschung der Daten mit der Begründung, dass die Veröffentlichung auf Anordnung des Ministeriums für Arbeit und Sozialordnung erfolgt sei. Im März 2010 legte Herr Gonzáles bei der spanischen Datenschutzbehörde Beschwerde gegen die Tageszeitung La Vanguardia sowie gegen Google Spain mit Sitz in Madrid und Google Inc. mit Sitz in Kalifornien ein. Er beantragte, die Zeitung anzuweisen, entweder die beiden Seiten zu löschen oder so zu ändern, dass seine personenbezogenen Daten dort nicht mehr erscheinen, oder mit den von der Suchmaschine zur Verfügung gestellten Werkzeugen dafür zu sorgen, dass sie nicht mehr in der Ergebnisliste angezeigt würden. Außerdem beantragte er, Google Spain und Google Inc. zu verpflichten, sicherzustellen, dass die ihn betreffenden Daten nicht weiter in den Suchergebnissen erscheinen und dazu führen, dass Links zu der Zeitung angezeigt werden.

Die spanische Datenschutzbehörde wies die Beschwerde gegen die Tageszeitung zurück, mit der Begründung, die Veröffentlichung sei rechtmäßig erfolgt. Dagegen gab sie der Beschwerde gegen Google Spain und Google Inc. statt und forderte die Unternehmen auf, die erforderlichen Maßnahmen zur Löschung der Daten aus ihrem Index zu ergreifen und einen künftigen Zugriff auf diese Daten unmöglich zu machen. Gegen diese Entscheidung haben Google Spain und Google Inc. bei dem zuständigen spanischen Gericht, der Audienca Nacional, jeweils Klage erhoben und die Aufhebung beantragt. Das nationale Gericht hat das Verfahren ausgesetzt und dem Europäischen Gerichtshof einige europarechtliche Fragen zur Vorabentscheidung vorgelegt, über die das Gericht mit Urteil vom 13. Mai 2014 entschieden hat.

2.6.2
Begründung

Der EuGH beschäftigt sich in seinem Urteil im Wesentlichen mit drei Themenbereichen:

1. dem sachlichen und räumlichen Anwendungsbereich der EG-Datenschutzrichtlinie,
2. dem Umfang der Verantwortlichkeit des Betreibers einer Internetsuchmaschine nach der EG-Datenschutzrichtlinie und
3. dem sog. Recht auf Vergessenwerden.

Die Tätigkeit einer Suchmaschine besteht darin, von Dritten ins Internet gestellte oder dort veröffentlichte, u. a. auch personenbezogene, Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen. Der EuGH sieht darin eine Verarbeitung personenbezogener Daten im Sinne der Datenschutzrichtlinie und in dem Betreiber der Suchmaschine den Verantwortlichen für die Verarbeitung, da er alleine über die Zwecke und Mittel der Datenverarbeitung entscheide.

Die räumliche Anwendbarkeit des europäischen Datenschutzrechts auf das in den USA ansässige Unternehmen Google Inc. rechtfertigt der EuGH mit der Existenz der Google-Niederlassungen in der EU. Er sieht darin die Voraussetzungen des Art. 4 Abs. 1 der EG-Datenschutzrichtlinie als erfüllt.

Art. 4 Abs. 1 EG-Datenschutzrichtlinie

Jeder Mitgliedstaat wendet die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an.

Recht kompliziert formuliert das Gericht: „Es ist davon auszugehen, dass die Verarbeitung personenbezogener Daten, die für den Dienst einer Suchmaschine wie Google Search erfolgt, die von einem Unternehmen betrieben wird, das seinen Sitz außerhalb der EU hat, jedoch in einem Mitgliedstaat der EU über eine Niederlassung verfügt, ‚im Rahmen der Tätigkeiten' dieser Niederlassung ausgeführt wird, wenn diese die Aufgabe hat, in dem Mitgliedstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine, mit denen die Dienstleistung der Suchmaschine rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen" (EuGH, C-131/12, Rdnr. 55). In diesem Fall ist nach Auffassung des Gerichts das nationale Recht des Mitgliedstaates, in dem die Niederlassung ihren Sitz hat, anzuwenden. Die Datenverarbeitung muss demnach keine unmittelbare Verbindung zur europäischen Niederlassung aufweisen, sondern es genügt, dass die Niederlassung zur Förderung der Rentabilität des Suchmaschinendienstes beiträgt.

Die Datenverarbeitung des Suchmaschinenbetreibers ist nach Ansicht des EuGH getrennt von der Datenverarbeitung, die auf der verlinkten Webseite erfolgt, zu bewerten. Die Wirkung des Eingriffs in das Grundrecht auf Achtung des Privatlebens und des Schutzes personenbezogener Daten durch die Webseite wird nach Meinung des EuGH durch Suchmaschinen noch gesteigert. Deshalb könne der Betreiber der Suchmaschine verpflichtet sein, Links zu von Dritten veröffentlichten Webseiten mit Informationen zu einer Person zu entfernen, obwohl die Veröffentlichung auf der Internetseite

rechtmäßig ist und kein direkter Löschungsanspruch gegen den Betreiber der Webseite besteht.

Die große öffentliche Resonanz erregte das Urteil dadurch, dass der EuGH gestützt auf die Grundrechtecharta der EU betroffenen Personen einen Anspruch gegen Suchmaschinenbetreiber eingeräumt hat, dass bestimmte Informationen über sie bei einer Suche anhand ihres Namens nach einer gewissen Zeit nicht mehr in der Ergebnisliste angezeigt werden. Dieses Recht besteht unabhängig davon, ob der Person durch die Einbeziehung der Information in die Trefferliste ein Schaden entsteht. Es kommt auch nicht darauf an, ob die Veröffentlichung auf der Quellenwebseite wahrheitsgemäß ist. Informationen und Links der Ergebnisliste müssen auf Antrag des Betroffenen gelöscht werden, wenn „die Informationen in Anbetracht aller Umstände des Einzelfalls den Zwecken der in Rede stehenden Verarbeitung durch den Suchmaschinenbetreiber nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen“ (EuGH, C-131/12, Rdnr. 94). Wie anhand dieses Maßstabs die Erstellung einer Ergebnisliste durch den Suchmaschinenbetreiber überhaupt unzulässig sein könnte, erschließt sich allerdings nicht, denn der Zweck der Datenverarbeitung besteht im Nachweis des Inhalts der Webseiten Dritter und dafür sind die Suchergebnisse immer erheblich.

Auch wenn der EuGH es nicht ausdrücklich so nennt, geht es hier um das im Zusammenhang mit der EU-Datenschutz-Grundverordnung (kontrovers) diskutierte Recht auf Vergessenwerden, das korrekterweise eher als „Recht, im Internet nicht gefunden zu werden“ bezeichnet werden müsste. Dieses Recht hat laut EuGH grundsätzlich Vorrang vor dem wirtschaftlichen Interesse des Suchmaschinenbetreibers und dem Interesse der breiten Öffentlichkeit am Zugang zu der Information. Der Suchmaschinenbetreiber kann die Entfernung des Eintrags aus der Ergebnisliste lediglich dann verweigern, wenn besondere Gründe, wie z. B. die Rolle des Betroffenen im öffentlichen Leben, ein überwiegendes Informationsinteresse einer breiten Öffentlichkeit rechtfertigen.

2.6.3
Folgen

Das Urteil wirft etliche Fragen auf, mit denen sich die Aufsichtsbehörden beschäftigen.

Unklar ist z. B., ob Google die beanstandeten Suchergebnisse nur auf der jeweiligen nationalen oder auf sämtlichen Domains und auf www.google.com entfernen muss. Bei einer nur nationalen Filterung besteht die Mög-

lichkeit der Umgehung, etwa durch Einsatz eines Proxys oder der Nutzung eines Tor-Netzwerks. Ein Anspruch auf weltweites Entfernen schafft allerdings ebenfalls ein großes Risiko, denn er könnte auch aus anderen Rechtsordnungen gegenüber Google geltend gemacht werden: So könnten russische Gerichte verlangen, dass Webseiten mit homosexuellen Inhalten aus der Trefferliste (weltweit) entfernt werden, iranische Gerichte könnten darauf bestehen, dass israelische Webseiten (weltweit) eliminiert werden. Am Ende könnte die Trefferliste löchrig wie ein berühmter Käse sein.

Zu präzisieren ist, welche Anforderungen Niederlassungen erfüllen müssen, um die Anwendbarkeit des nationalen Rechts auszulösen. Jedes Unternehmen, das seinen Sitz außerhalb der EU hat, aber Niederlassungen in Deutschland unterhält, die zur Rentabilität des Unternehmens beitragen, was fast immer der Fall sein dürfte, unterliegt nach der Rechtsprechung des EuGH nunmehr deutschem Datenschutzrecht und dem Recht der anderen Mitgliedstaaten, in denen es über Niederlassungen verfügt. Das könnte z. B. bereits der Fall sein, wenn das Unternehmen lediglich eine Lobbyeinrichtung in Deutschland unterhält.

Fraglich ist, welche Dienste außer Suchmaschinen das EuGH-Urteil noch erfasst. In Betracht kommen z. B. Wikipedia, Metasuchmaschinen, soziale Netzwerke oder auch nichtkommerzielle Suchmaschinen.

Dem Urteil sind kaum Kriterien für die Feststellung eines überwiegenden öffentlichen Interesses zu entnehmen, das einer Entfernung des Eintrags aus der Ergebnisliste entgegenstehen könnte. Bis auf den Hinweis, dass bei Personen des öffentlichen Lebens eine Beibehaltung des Eintrags gerechtfertigt sein könnte, finden sich keine weiteren Abwägungskriterien.

Umstritten ist auch, ob der Suchmaschinenbetreiber den Betreiber der Quellenwebseite auf eine Entfernung aus der Trefferliste informieren darf und auf eine erfolgte Löschung eines Eintrags in der Ergebnisliste hinweisen darf.

Das Urteil hat eine unvermeidliche wie unliebsame Konsequenz: Da der Suchmaschinenbetreiber den Eintrag aus der Trefferliste entfernen muss und ihn auch zukünftig nicht mehr anzeigen darf, muss er zwangläufig einen Index aller Quellen anlegen, die nicht angezeigt werden dürfen, mit anderen Worten einen Index der Beschwerdeführer und der Beschwerden. Das Urteil dürfte schließlich große kapitalstarke Betreiber von Suchmaschinen stärken. Es trifft besonders Personensuchmaschinen. Wie sich gerade in meinem Zuständigkeitsbereich gezeigt hat, haben die Betreiber kleinerer Suchmaschinen weder die personellen noch finanziellen Mittel, um eine gründliche Prüfung der Löschungsanträge vorzunehmen, sondern entsprechen ohne Prüfung des Einzelfalls dem Löschungsverlangen.

3. Übergreifende Themen (öffentlicher und nicht öffentlicher Bereich)

3. Querschnittsthemen

3.1.1 Umgang mit Patientendaten nach Schließung von Krankenhäusern

Bei der Schließung von Krankenhäusern, insbesondere in Fällen von Insolvenz, gibt es ein hohes Risiko, dass die Patientenakten nicht sicher verwahrt werden oder die Verwahrung bzw. Vernichtung nicht mehr sichergestellt wird. Vor dem Hintergrund aktueller Fälle in Hessen habe ich das Hessische Ministerium für Soziales und Integration kontaktiert. Gemeinsam mit der Landesärztekammer Hessen, der Hessischen Krankenhausgesellschaft, dem Berufsverband der in Deutschland tätigen Insolvenzverwalter und weiteren Stellen sollen praktikable Regelungen und Problemlösungen entwickelt werden.

Im Mittelpunkt meiner datenschutzrechtlichen Prüfung standen Fragen zum Verbleib und zur ordnungsgemäßen Aufbewahrung der Patientendokumentation.

3.1.1.1 Geschlossene Asklepios-Klinik in Homberg (Efze)

3.1.1.1.1 Sachverhalt

Über den Sachverhalt wurde meine Dienststelle erstmals im April 2014 durch eine Eingabe sowie Zeitungsartikel in der lokalen Presse informiert. Wie daraus hervorging, soll eine Person auf einer Wiese im Umfeld der Klinik eine Krankenakte gefunden haben. Daraufhin bestätigte die Polizei, dass es vermutlich zu einem Einbruch in dem leerstehenden Komplex in Homberg (Efze) gekommen sei. Auch ein Strahlendosimeter wurde im Umfeld der Klinik gefunden. Noch in der gleichen Woche erfolgte eine Begehung der Klinik durch meine Dienststelle in Begleitung der Geschäftsführung des Hauses (Asklepios Schwalm-Eder-Kliniken GmbH) sowie der örtlich zuständigen Polizei.

Bei dieser ersten Begehung wurde festgestellt, dass die Patientendaten nicht ordnungsgemäß gesichert waren. Beispielhaft seien hier die folgenden Mängel benannt:

– Die Eingangstür und sämtliche Fenster waren nicht gegen Einbruch geschützt,
– die in verschiedenen Räumen vorgefundenen medizinischen Unterlagen (Akten, Festplatten, Röntgenbilder) wurden zum Teil in unverschlossenen Schränken aufbewahrt,
– zwei Archivräume im Keller hatten keine einbruchhemmenden Türen.

In diesem Kontext stellte sich heraus, dass es sich anders als in dem Fall des Rehazentrums im Urbachtal (s. Ziff. 3.1.1.2) um eine geplante Schließung handelte. Die Klinik hatte die Räumlichkeiten bereits seit 2010 nicht mehr in vollem Umfang genutzt. Ende 2013 wurde der Betrieb aus Gründen der fehlenden Wirtschaftlichkeit vollends eingestellt.

3.1.1.1.2
Unsere Forderungen/Getroffene Maßnahmen

Bei der Begehung konnte festgestellt werden, dass eine ausreichende Außenhautsicherung des leerstehenden und abgelegenen Gebäudekomplexes praktisch nicht vorhanden war. Eingangstüren und Fenster waren nicht gegen Einbruch geschützt. Die nach § 10 Abs. 2 HDSG zu fordernden Maßnahmen waren somit nicht erfüllt.

Als Sofortmaßnahmen wurden daher die folgenden Punkte gefordert:

– Verbringung der zusammengetragenen Akten, Festplatten und Röntgenbilder, die noch einer Aufbewahrungspflicht unterliegen, in Archivräume im leerstehenden Gebäude,
– Sicherung der Türen und Fenster dieser Räume mittels besonderer Vorrichtungen und
– ordnungsgemäße Vernichtung der Daten, die bereits einer Vernichtung zuzuführen sind.

Hierbei handelte es sich zunächst nur um das kurzfristige Sicherungskonzept. Zudem wurde die Erstellung eines umfassenden Gesamtsicherheitskonzeptes gefordert.

Da die Geschäftsführung keine Möglichkeit sah, die Akten in ihren anderen, noch weiter betriebenen Kliniken unterzubringen, entschloss sie sich, den Komplex als langfristige Lagerungsstätte vorzusehen. Hierzu hat die örtliche Polizei ein entsprechendes Sicherungskonzept vorgeschlagen. Aufgrund der relativ abgeschiedenen Lage des Objekts in Verbindung mit dem faktischen Leerstand des Gebäudes wurde von dort empfohlen, zur möglichst sicheren Verwahrung der Krankenakten eine Kombination aus mechanischem Grundschutz in Verbindung mit einer elektronischen Absiche-

rung durch die zusätzliche Installation einer Einbruchmeldeanlage einzurichten.

In einer Nachbesichtigung im Mai wurden die kurzfristigen Sicherungsmaßnahmen durch meine Dienststelle in Augenschein genommen. Zudem wurde auch die Situation vor Ort in einer der aktiven Kliniken der Asklepios Schwalm-Eder-Kliniken GmbH überprüft. Der Verdacht, dass das in Homberg Vorgefundene auf Mängel in den anderen, noch aktiven Krankenhäusern der Asklepios Schwalm-Eder-Kliniken GmbH schließen lässt, hat sich dabei nicht erhärtet.

Die Umsetzung der langfristigen Sicherungsmaßnahmen wurde mir gegenüber mittlerweile zum Juli 2014 angezeigt.

3.1.1.1.3
Grundsätzliche Überlegungen/Rechtsfragen für die Zukunft

Den Vorfall habe ich zum Anlass genommen, um auch noch einmal das Hessische Ministerium für Soziales und Integration (HSM) zum Sachverhalt zu befragen. Dieses war in die geplante Schließung der Klinik mit eingebunden. Von dort wurde mitgeteilt, dass es derzeit bei einer geplanten Schließung nicht vorgesehen ist, dass ein Konzept betreffend die künftige Aufbewahrung und Lagerung von Patientenakten vorgelegt wird. Man könne sich jedoch vorstellen, dass aufgrund des aktuellen Vorfalles Regelungen geschaffen werden, die dies vorsehen.

Ergänzend hierzu wurde seitens des HSM mitgeteilt, dass für diese Legislaturperiode eine Fortentwicklung des Hessischen Krankenhausgesetzes beabsichtigt ist.

In die Überlegung hierzu werde man auch aufnehmen, ob in Hessen eine Regelung umgesetzt werden sollte, wie es sie beispielsweise bereits in Berlin gibt. Angesprochen wurde insoweit § 41 der Berliner Krankenhausverordnung.

> *§ 41 Berliner KhsVO*
>
> *Bei Schließung oder Umwandlung eines Krankenhauses oder eines Teils davon in eine Pflege- oder Betreuungseinrichtung wird die Patientendokumentation abgeschlossen. Die weitere Aufbewahrung des Bestandes an Patientendokumentationen wird vom Krankenhausträger im Einvernehmen mit dem zuständigen Bezirksamt so geregelt, dass Unbefugte nicht Einsicht nehmen können.*

Aus meiner Sicht müssten darüber hinaus aber auch Regelungen für den Fall getroffen werden, dass kein Ansprechpartner des Krankenhauses mehr

vorhanden ist und ehemalige Patienten ihre Akte einsehen möchten und/oder die Akten für die Weiterbehandlung benötigt werden. Entsprechendes habe ich auch dem HSM als zuständige Aufsichtsbehörde mitgeteilt. Dies ist auch ein Aspekt, der den Zuständigkeitsbereich der Landesärztekammer tangiert. Hier ist insoweit noch völlig offen, wer genau in Hessen in diesen Konstellationen nach welchen Grundsätzen die Akteneinsicht gewähren darf. Eine ähnliche Fragestellung ergibt sich für die, nach einem entsprechenden Zeitraum vorzunehmende, Vernichtung der Akten.

Ferner ist auch zu berücksichtigen, dass nicht alle betroffenen Einrichtungen unter das Landeskrankenhausgesetz fallen. Es besteht insoweit auch noch ein zusätzlicher Regelungsbedarf, da der Anwendungsbereich des Landeskrankenhausgesetzes in Hessen keine Rehabilitations- und Vorsorgekliniken erfasst. Auch bei Privatkliniken gibt es Ausnahmen. Ein möglicher Ansprechpartner in diesem Zusammenhang ist der Landesverband der Privatkliniken in Hessen und Rheinland-Pfalz e. V. (VDPK), der auch für die Interessenvertretung von Rehakliniken zuständig ist.

Die Thematik dürfte im Übrigen bundesweit alle Länder betreffen. Bei Internetplattformen wie Youtube sind vielfach Aufnahmen von leerstehenden Krankenhäusern in Deutschland zu finden. Inwieweit darin noch Patientenakten untergebracht sind, ist auf den Aufnahmen nicht zu erkennen.

3.1.1.2
Ehemalige Reha-Klinik im Urbachtal (Neukirchen, Hessen)

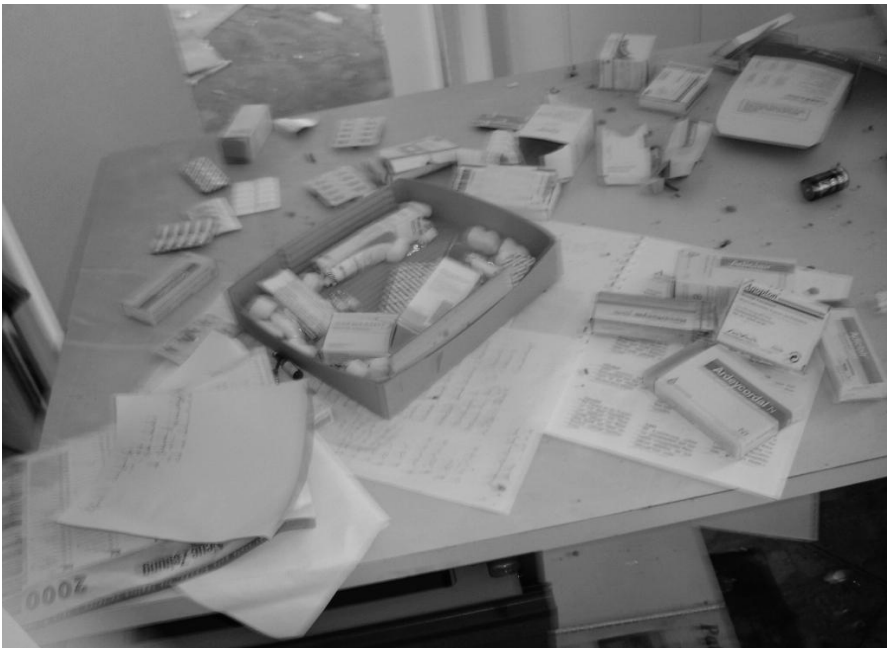
3.1.1.2.1
Sachverhalt

Meine Dienststelle wurde erstmals im Oktober 2013 durch eine anonyme Eingabe darauf aufmerksam gemacht, dass in einer ehemaligen Reha-Klinik im Urbachtal (Neukirchen, Hessen) nach wie vor Akten von ehemaligen Patienten untergebracht sind. Aufgrund dieses Verdachts wurde die örtliche Polizeistation in Schwalmstadt gebeten, das Objekt zu begehen und sich ein Bild von der Lage zu machen.

Aus dem daraufhin erstellten Bericht der Polizeistation Schwalmstadt geht hervor, dass das Objekt seit Jahren regelmäßig Ziel von Vandalismus und Diebstählen ist, insbesondere mit der Zielrichtung Altmetall. Aufgebrochene Zugangstüren und Fenster würden einen mehr oder minder ungehinderten Zugang in die Gebäude zulassen.

Es wurde zudem bestätigt, dass noch erhebliche Mengen an Patienten- und Personalakten in dem Objekt vorhanden sind. Diese waren zum Teil


1933



hinter verschlossenen Türen gesichert, zum Teil aber auch auf den Fluren verteilt.

Wie weiterhin mitgeteilt wurde, seien die lose verstreuten Patienten- und Personalakten in einem separaten Aktenraum mit massiver und unbeschädigter Zugangstür untergebracht worden.

Weitere Recherchen ergaben, dass der Betrieb des Reha-Zentrums bereits Ende 2002 eingestellt wurde und seit dieser Zeit ein Insolvenzverfahren anhängig ist.

3.1.1.2.2
Meine Forderungen und getroffene Maßnahmen

Im Anschluss daran kontaktierten meine Mitarbeiter verschiedene Stellen, um abzuklären, wie die langfristig sichere Aufbewahrung und ggf. Vernichtung der Akten gewährleistet werden kann, ebenso wie die Herausgabe der Akten im Falle einer notwendigen Weiterbehandlung. Hierzu wurden die LÄK Hessen, das Hessische Ministerium der Justiz, das Hessische Sozialministerium sowie der Insolvenzverwalter der Klinik angeschrieben.

Der Insolvenzverwalter teilte mit, dass das Insolvenzverfahren noch nicht beendet sei und es zu seinen Aufgaben zählt, für eine sichere Verwahrung/Vernichtung der Akten zu sorgen. Zugleich wurde jedoch darauf verwiesen, dass keine ausreichende Masse mehr vorhanden sei, um die sensiblen Daten in ordnungsgemäßer Weise zu lagern/zu vernichten.

Im Juli 2014 gab es erneut eine Eingabe bzgl. des Reha-Zentrums.

Diesmal war hierbei der Hintergrund, dass der Eingebende die Akte seines verstorbenen Sohnes, der in der Klinik behandelt worden war, in sichere Verwahrung nehmen wollte. Zu diesem Zweck suchte der Eingebende das Objekt mit der örtlichen Polizei auf. Die Akte wurde nicht aufgefunden. Die vorgefundene Situation gab erneut Anlass dazu, meine Dienststelle zu kontaktieren. Auch die lokale Presse berichtete mehrfach über den Fall.

Es fand kurze Zeit darauf ein Ortstermin statt, an dem neben meinen Mitarbeitern die örtliche Polizei, das Ordnungsamt, der Insolvenzverwalter sowie der ehemalige Hausmeister des Objekts teilnahmen.

Bei dieser Begehung konnten erneut Dokumente aus Behandlungen von Patienten sowie Dokumente von Beschäftigten in offenen Bereichen aufgefunden werden. Nicht sicher geklärt werden konnte, ob diese erneut aus den Räumlichkeiten entwendet wurden, in denen diese zuvor untergebracht worden waren. Aufgrund der abgelegenen Lage des Objekts war jedoch klar erkennbar, dass man sich ohne Weiteres ungestört Zugang in das Gebäude verschaffen konnte.

Die örtliche Polizei und das Ordnungsamt sahen hier zunächst den HDSB in der Pflicht, vor Ort die notwendigen Maßnahmen zur Abwendung von Gefahren im Hinblick auf § 203 StGB zu treffen.

Seitens meiner Dienststelle wurde jedoch darauf verwiesen, dass der Datenschutzbeauftragte nur entsprechende Zustände feststellen und ggf. mittels Bußgeldtatbeständen ahnden kann. Es besteht für ihn jedoch keine Möglichkeit, quasi im Sofortvollzug eine Ersatzvornahme durchzuführen. Die örtlich zuständige Polizei und das Ordnungsamt erklärten sich daraufhin dazu bereit, die Unterlagen in verschließbaren Räumlichkeiten im Objekt unterzubringen. Hierzu wurden Mitarbeiter des Bauhofs Neukirchen eingeschaltet, welche die im Gebäude verstreuten Dokumente in dafür geeigneten, verschließbaren Räumen des Gebäudekomplexes unterbrachten.

Da sich unter den Unterlagen auch Röntgenbilder befanden, wurde ferner das RP Kassel eingeschaltet. Soweit dies den Zuständigkeitsbereich „Röntgenbilder“ betrifft, führte das RP Kassel als für die Röntgenverordnung zuständige Behörde hierzu aus:

Unsere Anordnungsbefugnis ergibt sich aus § 28 Abs. 3 Satz 4 RöV und im Übrigen aus § 33 Abs. 2 RöV. Adressat der Anordnung nach § 28 Abs. 3 Satz 4 RöV ist der Strahlenschutzverantwortliche, da diesem die Aufbewahrungspflicht obliegt. Anordnungen nach § 33 Abs. 2 RöV sind gem. § 33 Abs. 4 Satz 1 – ausschließlich – an den Strahlenschutzverantwortlichen zu richten. Der Insolvenzverwalter ist jedoch nicht Strahlenschutzverantwortlicher. Er ist auch niemals Strahlenschutzverantwortlicher gewesen, da der Betrieb der Röntgenanlage zum Zeitpunkt des Beginns seiner Tätigkeit bereits eingestellt war. Der Übergang der Verwaltungs- und Verfügungsbefugnis (auch an den Röntgenbildern und Aufzeichnungen nach § 28 Abs. 1 RöV) auf den Insolvenzverwalter bewirkt daher keine Ordnungspflicht desselben nach dem speziellen Ordnungsrecht der RöV, da dieses die Stellung als Strahlenschutzverantwortlicher voraussetzt.

Auch eine Anordnung gegenüber der in der Insolvenz befindlichen GmbH & Co. KG als Strahlenschutzverantwortliche scheidet nach den Ausführungen des RP Kassel aus, da diese aufgrund der Insolvenz nicht befugt ist, der Anordnung nachzukommen. Aus Sicht des RP Kassel bleibt daher nur die Möglichkeit, Anordnungen nach dem allgemeinen Polizei- und Ordnungsrecht zu treffen, für die das RP Kassel nicht zuständig ist.

In einem Polizeibericht vom Juli dieses Jahres wurden noch einmal langfristige Sicherungsempfehlungen bekannt gegeben. Diese dürften angesichts der Größe des Objekts jedoch sehr aufwendig und kostenintensiv sein. Es wird insoweit ähnlich wie bereits bei der Klinik in Homberg eine Kombination aus mechanischem Grundschutz in Verbindung mit einer elektronischen Absicherung durch die zusätzliche Installation einer Einbruchmelde-

anlage empfohlen. Alternativ wäre laut Polizei eine Auslagerung in eine aus Datenschutzgesichtspunkten sichere Örtlichkeit zu empfehlen. Eine Sicherung des Objekts scheidet aus Sicht des HDSB jedoch, anders als im Falle der Asklepios-Klinik in Homberg (Efze), wohl bereits deshalb aus, weil keine entsprechende Infrastruktur mehr im Objekt vorhanden ist. So gibt es dort insbesondere keine Stromversorgung mehr.

Zwischenzeitlich hat die Deutsche Rentenversicherung (DRV Bund) ihr Interesse angekündigt, für eine Lösung des Problems zu sorgen. Der Hintergrund hierfür ist, dass die DRV Bund bis zum 28. Februar 2002 die Reha-Klinik als Vertragshaus mit Patienten belegt hat.

Die Patientenakten wurden inzwischen mit der Vernichtung einer – aus Sicht der DRV Bund – datenschutzgerechten Lösung zugeführt. Man geht davon aus, dass hierfür eine Aufbewahrungsfrist von zehn Jahren vorgesehen war, die inzwischen verstrichen ist. Die BfDI hat im Hinblick auf dieses Vorgehen keine Einwände erhoben.

Aufgrund des Vorfalls wird die DRV Bund auch die Vertragskrankenhäuser für die Thematik sensibilisieren. Man will darauf hinwirken, dass bereits jetzt, für den Fall einer Einstellung des Betriebes, ein entsprechendes Konzept im Hinblick auf die Patientendokumentation vorliegt.

3.1.1.2.3
Grundsätzliche Überlegungen/Rechtsfragen für die Zukunft

Der Vorgang zeigt, dass es insbesondere im Falle der Insolvenz einer Klinik ein hohes Risiko gibt, dass Patientenakten nicht sicher verwahrt werden und die Verwahrung/Vernichtung/Herausgabe nicht mehr sichergestellt wird. Dies droht vor allem für den Fall, dass nicht mehr ausreichend finanzielle Mittel aus der Insolvenzmasse zur Verfügung stehen. Der Insolvenzverwalter bleibt zwar für die Patientenakten verantwortlich, er ist in diesen Fällen jedoch handlungsunfähig. Insbesondere kann er keine Aufträge zur Sicherung der Akten vergeben, da er ansonsten einen Auftrag vergeben würde, in dem Wissen, die dabei entstehenden Kosten nicht begleichen zu können (möglicherweise strafbar als Eingehungsbetrug).

Vor diesem Hintergrund fand Ende dieses Jahres ein Gespräch im Hessischen Ministerium für Soziales und Integration statt. Zu diesem Gespräch waren u. A. die Landesärztekammer Hessen, die Hessische Krankenhausgesellschaft, der Landesverband der Privatkliniken in Hessen, der Zentralverband Ambulanter Therapieeinrichtungen e. V. sowie der Berufsverband der in Deutschland tätigen Insolvenzverwalter eingeladen. Bei diesem Gespräch wurde mit hoher Mehrheit ein Regelungsbedarf festgestellt. Es

wurde daher vereinbart, dass die anwesenden Kammern und Verbände bis Anfang nächsten Jahres Lösungsansätze an das Ministerium übermitteln. Es wird dann eine erneute Zusammenkunft geben, bei welcher die Lösungsvorschläge zur Diskussion gestellt werden. Angedacht ist beispielsweise eine Fonds-Lösung, in der betroffene Einrichtungen verpflichtet werden, finanziell für entsprechende Fälle vorzusorgen. Als Ansatzpunkt sollen aber auch bereits bestehende gesetzliche Regelungen dienen, wie beispielsweise der § 39 Abs. 6 des Landeskrankenhausgesetzes Mecklenburg-Vorpommern.

§ 39 Abs. 6 LKHG M-V

Übernimmt ein Auftragnehmer nach einer Betriebseinstellung eines Krankenhauses den gesamten Bestand der Patientendaten, gelten für ihn als verantwortliche Stelle hinsichtlich der Verarbeitung dieser Daten die Vorschriften dieses Abschnitts. Bei der Übernahme ist vertraglich sicherzustellen, dass die Patientinnen und Patienten für die Dauer von zehn Jahren nach Abschluss der Behandlung oder Untersuchung auf Verlangen in gleicher Weise wie bisher beim Krankenhaus Auskunft und Einsicht erhalten.

3.1.2
Weiter in der Diskussion: Ausgestaltung der Zugriffsberechtigungen in Krankenhausinformationssystemen

2014 wurde die Orientierungshilfe für Krankenhausinformationssysteme von den Datenschutzbeauftragten aktualisiert. Meine Prüfungen vor Ort habe ich fortgesetzt. Probleme habe ich insbesondere festgestellt hinsichtlich der verbindlichen Festlegung der Abläufe bei der Protokollierung und deren Umsetzung.

3.1.2.1
Aktualisierung der „Orientierungshilfe Krankenhausinformationssysteme“

Seit dem Jahr 2011 gibt es als Reaktion auf bundesweit festgestellte Defizite bei Krankenhausinformationssystemen die von den Datenschutzbeauftragten des Bundes und der Länder erstellte Orientierungshilfe für Krankenhausinformationssysteme (OH KIS). Nach den bei Prüfungen vor Ort und in Diskussionen gesammelten Erfahrungen aus den letzten Jahren wurde die erste Fassung der OH KIS aktualisiert und in der jetzt vorliegenden zweiten Fassung im März 2014 veröffentlicht (https://www.datenschutz.hessen.de/ft-gesundheit.htm). Mit dieser aktualisierten Version der Orientierungshilfe werden keine neuen Themenbereiche erschlossen oder

die Anforderungen der Ursprungsfassung revidiert, sondern insbesondere notwendige Klarstellungen bzw. Konkretisierungen der Anforderungen vorgenommen. So wurde, um Verständnisschwierigkeiten zu begegnen, z. B. der Teil I (Rechtliche Rahmenbedingungen) weiter präzisiert. Speziell für einrichtungs- und mandantenübergreifende Zugriffe wurde zusätzlich ein Szenarienkatalog bereitgestellt. In Teil II (Technische Anforderungen) der Orientierungshilfe wurde der durchgehende Bezug zu den rechtlichen Rahmenbedingungen verdeutlicht. Insgesamt wird nun noch deutlicher, dass den rechtlichen Anforderungen durch verschiedenartige System- und Prozessgestaltung entsprochen werden kann.

3.1.2.2
Ergebnisse der Prüfungen im Berichtszeitraum

Wie in den vergangenen Jahren habe ich meine stichprobenhaften Prüfungen von Krankenhausinformationssystemen in hessischen Krankenhäusern fortgesetzt.

Positiv festzustellen war, dass auch bei den im letzten Jahr geprüften Kliniken ein großer Teil der Orientierungshilfe umgesetzt wurde. So haben die geprüften Krankenhäuser alle ein differenziertes Rollen- und Berechtigungskonzept erstellt. In dem Berechtigungskonzept wird nach Benutzergruppen differenziert. Jeder Benutzergruppe werden Gruppenrechte zugeordnet und darüber hinaus werden teilweise zur genaueren Differenzierung individuelle Rechte an einzelne Benutzer vergeben. Differenziert wird bei der Rechtevergabe nach Standardzugriffsberechtigungen und erweiterten Zugriffsberechtigungen in besonderen Situationen (z. B. sog. Sonderuserzugriffsberechtigung für Notfälle). Sammelkennungen wurden in der Regel nicht mehr eingesetzt. Interne Datenschutzbeauftragte waren bestellt und wurden in die Diskussionen über die datenschutzrechtlichen Anforderungen in der Klinik regelmäßig einbezogen.

Probleme gab es offenbar bei der Festlegung der Abläufe, bei der Protokollierung von Zugriffen und der Auswertung der Protokolle:

Bei meinen Prüfungen konnte ich feststellen, dass ein Großteil der KIS-Systeme technisch durchaus in der Lage ist, den Zugriff auf Patientendaten zu protokollieren, die Krankenhäuser jedoch kein hinreichendes Konzept im Umgang mit der Protokollierung hatten. So existierte meist keine verbindliche schriftliche Festlegung von Umfang und Zweck der Protokollierung und den Abläufen bei der Auswertung der Protokolle. Es gab auch keine geeignete technische Auswertungsmöglichkeit für die im KIS anfallenden Protokolldaten.

Grundsätzlich ist die Protokollierung im Gesamtzusammenhang mit der Ausgestaltung der Zugriffsberechtigungen zu sehen. In der Regel sind in gewissem Umfang Pauschalierungen bei der Ausgestaltung nicht zu vermeiden. Umso wichtiger ist eine Erstellung von Zugriffsprotokollen und deren Auswertung. Je weitreichender die Zugriffsrechte im KIS ausgestaltet sind, desto wichtiger sind die Protokolle und deren routinemäßige Auswertung. Mit der Etablierung der Protokollierung und der regelmäßigen Auswertung wird Datenschutzverstößen von vornherein präventiv entgegengewirkt, wenn die Mitarbeiter über die Maßnahmen informiert sind. Zudem kann damit erkannten Unregelmäßigkeiten nachgegangen werden.

Die Protokollierung von Zugriffen auf Patientendaten ist daher kein Selbstzweck. Sie erfüllt nur dann ihren Zweck, wenn die Protokolle auch tatsächlich ausgewertet werden. Die Protokolldaten dienen zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung und zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen (§ 10 Abs. 2 HDSG).

Im Rahmen der vorbeugenden Datenschutzkontrolle sind die Protokolle turnusmäßig auf bestimmte Auffälligkeiten hin wie z. B. auffällige Häufungen von Abfragen unter bestimmten Benutzerkennungen, eine Häufung von Abfragen außerhalb der Dienstzeiten oder mit unüblichen Suchkriterien oder auch klärungsbedürftige Begründungen für die Verwendung von Sonderuserberechtigungen hin auszuwerten.

Bei einem hinreichend fein differenzierten Zugriffsschutz im KIS kann die Protokollierung und auch die Auswertung der Protokolle reduziert werden. Umgekehrt steigt jedoch ihre Bedeutung in den Bereichen, in denen mit sehr weit gefassten Zugriffsberechtigungen gearbeitet wird. Wird der Mitarbeiter nur im Rahmen seiner regulären Zugriffsberechtigung (z. B. lesender Zugriff auf die Daten von Patienten seiner Fachabteilung) tätig, ist es ausreichend, wenn allein bei Verdacht auf Missbrauch eine Prüfung der Protokolldaten erfolgt. Sind im KIS jedoch – wie es üblicherweise der Fall ist – Möglichkeiten vorgesehen, die es den Mitarbeitern erlauben, einen erweiterten Zugriff über die reguläre Zugriffsberechtigung hinaus zu erhalten (Notfallzugriff, Konsil, Mandantenwechsel etc.), reicht die alleinige Prüfung bei Verdacht auf Missbrauch nicht aus, sondern es ist zusätzlich in **regelmäßigen Abständen** zu prüfen, ob der erweiterte Zugriff berechtigt im Rahmen der dienstlichen Aufgabe erfolgte (s. a. Teil I, Punkt 45 OH KIS).

Dazu ist ein Protokollierungs- und Auswertungskonzept zu erstellen, in dem auch Auffälligkeits- und Stichprobenauswertungen der Zugriffsprotokolle in einer angemessenen Prüfdichte vorzusehen sind.

§ 13 Abs. 5 HDSG sieht für die anfallenden Protokolldaten eine strikte Zweckbindung vor, keinesfalls dürfen die Daten für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden (§ 34 Abs. 6 HDSG). Um dies sicherzustellen, sind auch Beteiligungsrechte der Personalvertretung hinsichtlich der Details der Ausgestaltung der Abläufe und der daran Beteiligten zu beachten. So kann ein transparentes Verfahren erreicht werden, das alle Interessen berücksichtigt. Weitere Hinweise bietet auch die Orientierungshilfe „Protokollierung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahr 2009 (https://www.datenschutz.hessen.de/tf012.htm).

Die Art und Weise der Umsetzung meiner Forderungen wird 2015 Gegenstand weiterer Gespräche mit den betroffenen Krankenhäusern sein.

3.2
Entwicklungen und Empfehlungen im Bereich der Technik

3.2.1
Technischer Datenschutz und IT-Sicherheit – Aktivitäten in 2014

Fragen der IT-Sicherheit stoßen zunehmend auf öffentliches Interesse.

Vor allem als Reaktion auf die NSA-Affäre hat die Nachfrage nach Beratungen auf dem Gebiet des technischen Datenschutzes spürbar zugenommen. Gegenüber den gelegentlichen resignativen Feststellungen, wegen Umfang und Tiefe der nachrichtendienstlichen Eingriffe seien Schutzvorkehrungen faktisch nutzlos, habe ich immer wieder darauf hingewiesen, dass die verfügbaren technischen Sicherheitsmaßnahmen gleichwohl sinnvoll sind. Dies gilt für den öffentlichen und privaten Bereich.

3.2.1.1
Aktivitäten der Hessischen Landesverwaltung

So teile ich im Ansatz das Sicherheitskonzept, das von der Hessischen Landesverwaltung umgesetzt wird. Durch eine Vielzahl von Maßnahmen wurde ein Prozess zur Verbesserung der IT-Sicherheit etabliert. Bereits im Jahr 2004 wurden eine IT-Sicherheitsleitlinie in Kraft gesetzt (StAnz 2004, S. 3827 f.) und ein Arbeitskreis zur IT-Sicherheit eingerichtet (vgl. meinen 33. Tätigkeitsbericht, Ziff. 8.2). Die Leitlinie wurde fortgeschrieben und mit Wirkung vom 1. Januar 2010 trat sie als „Informationssicherheitsleitlinie für die Hessische Landesverwaltung“ in Kraft (StAnz 2010, S. 106 ff.). Eine Vorgabe ist, dass es in hessischen Behörden nicht nur einen IT-Sicherheitsbe-

auftragten gibt, sondern auch ein IT-Sicherheitsmanagementteam und einen Prozess, um die IT-Sicherheit zu gewährleisten. Diese und weitere Maßnahmen sind flächendeckend in Hessen eingeführt. Der o. g. Arbeitskreis ist weiterhin tätig und es werden dort Fragen behandelt, die im Zusammenhang mit der IT-Sicherheit der Landesverwaltung relevant sind; in der Gremienstruktur des Landes ist er das Fachgremium zu diesem Thema.

Parallel dazu wurde das CERT Hessen eingerichtet (CERT: Computer Emergency Response Team). Vom CERT Hessen werden aktuelle Sicherheitswarnungen und Sicherheitsvorfälle analysiert und den Behörden der Landesverwaltung und angeschlossenen Kommunen Hinweise gegeben oder auch Lösungsvorschläge gemacht. Es ist in einem Verbund tätig, zu dem das BSI für die Bundesverwaltung und andere Bundesländer gehören. Derzeit wird überlegt, ob die Informationen auch anderen Stellen wie kleinen Firmen zur Verfügung gestellt werden können.

Länderübergreifend hat sich Hessen auch auf dem Gebiet der Cybersicherheit engagiert. Neben einem internen Arbeitskreis wurde auf Bundesebene eine Arbeitsgruppe ins Leben gerufen, die sich mit den zugehörigen Themen befasst.

Noch über das ersichtliche Engagement hinaus hat die Landesregierung Ende 2013 auf meinen Vorschlag hin entschieden, eine Untersuchung durchzuführen, wie die Informationssicherheit auf Landesebene optimiert werden kann. Auch wenn der Auslöser für diese Untersuchung die Enthüllungen von Snowden war, ist das Ziel der Untersuchung breiter angelegt; es geht darum, alle Aspekte zu prüfen. Zuerst wurde durch eine Arbeitsgruppe ein Katalog von Handlungsfeldern bestimmt. Darauf aufbauend wurden Prioritäten gesetzt und acht vorrangig zu behandelnde Themen benannt. Dieser Vorschlag wurde dem CIO, der auch Finanzminister ist, und dem Innenminister vorgestellt. Diese nahmen den Vorschlag auf und erteilten den Auftrag, in Form von Projekten die Themen zu bearbeiten. Im Herbst 2014 fiel der Startschuss für die Projekte. Im Rahmen meiner Möglichkeiten werde ich die Projekte begleiten.

Ich glaube, dass die Hessische Landesverwaltung auf einem guten Weg ist, eine angemessene IT-Sicherheit zu erreichen und auch langfristig sicherzustellen.

3.2.1.2
Sonstige Sicherheitsprobleme am Beispiel SSL-Verschlüsselung

Neben der NSA-Affäre gab es in 2014 eine Reihe von Meldungen über IT-Sicherheitslücken mit teilweise erheblichen Konsequenzen für datenverar-

beitende Stellen. Exemplarisch möchte ich hier Fälle im Zusammenhang mit SSL resp. TLS nennen, mit denen ich mich intensiver befasst habe.

SSL (Secure Sockets Layer; erste Version 1994) und der Nachfolger TLS (Transport Layer Security; SSL Version 3.1 entspricht TLS Version 1.0, seit 1999) sind Protokolle zur verschlüsselten Übertragung von Daten im Internet.

Verschlüsselung kommt im Internet immer dann zum Einsatz, wenn der Nachrichtenaustausch vertraulich stattfinden soll, z. B. beim Homebanking. Zu diesem Zweck wird derzeit SSL, oder besser TLS, genutzt.

3.2.1.2.1
Zu den grundsätzlichen Abläufen

Verschlüsselung und Entschlüsselung

Durch Verschlüsselung wird eine offene Nachricht (Klartext) in eine verschlüsselte Nachricht (Geheimtext) transformiert. Im Idealfall lässt der Inhalt der verschlüsselten Nachricht keine Rückschlüsse auf den Inhalt der unverschlüsselten Nachricht zu. Für die Transformation wird ein Verschlüsselungsalgorithmus verwendet, der als Parameter einen Schlüssel benötigt.

Eine Entschlüsselung ist die umgekehrte Transformation. Die verschlüsselte Nachricht wird in die ursprüngliche – offene – Nachricht umgewandelt. Dazu wird ein Entschlüsselungsalgorithmus mit einem Schlüssel als Parameter verwendet. Verschlüsselungs- und Entschlüsselungsalgorithmus inkl. zugehöriger Schlüssel können, müssen aber nicht gleich sein. Eine Entschlüsselung ohne Kenntnis des Schlüssels darf nur mit erheblichem Aufwand möglich, im Idealfall unmöglich sein.

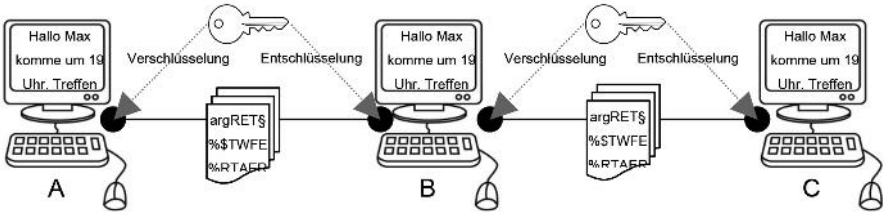
Ende-zu-Ende-Verschlüsselung

Bei der Ende-zu-Ende-Verschlüsselung wird die Nachricht vom Absender so verschlüsselt, dass sie nur der Empfänger mit seinem bzw. dem geheimen Schlüssel entschlüsseln kann.

Vorteil ist, dass bei der Übertragung die Nachricht auf keinem Rechner im Klartext vorliegt. Nachteil ist, dass sich Absender und Empfänger auf ein Verschlüsselungsverfahren und Schlüssel einigen müssen. Hat die Vertraulichkeit der Nachricht Priorität, muss eine Ende-zu-Ende-Verschlüsselung mit starken Verschlüsselungsverfahren (Algorithmen, Schlüssel) genutzt werden. Zur E-Mail-Verschlüsselung wird beispielsweise PGP (Pretty Good Privacy) verwendet, bei dem starke Algorithmen mit sicheren Schlüssellängen verwendet werden können.

Punkt-zu-Punkt-Verschlüsselung (Leitungsverschlüsselung)

Die Nachricht wird auf der Leitung zwischen zwei Rechnern verschlüsselt. Auf den Rechnern selbst sind die Nachrichten unverschlüsselt. Rechner A verschlüsselt für Rechner B, der entschlüsselt und verschlüsselt für Rechner C usw.



Falls also der Absender am Rechner A seine Nachricht schreibt und über den Rechner B an den Empfänger schickt, der den Rechner C benutzt, so liegt bei einer Leitungsverschlüsselung die Nachricht auf B unverschlüsselt vor. Vorteil ist, dass nur die miteinander kommunizierenden Rechner sich auf einen Verschlüsselungsalgorithmus und einen Schlüssel einigen müssen. Ein Nachteil ist, dass die Nachricht auf ihrem Wege auf B im Klartext vorliegt. Man muss folglich darauf vertrauen, dass auf B keine unbefugten Zugriffe erfolgen.

Das Verfahren wird gerne im Internet eingesetzt, um von einem Browser eine SSL- resp. TLS-verschlüsselte Verbindung (https – HyperText Transfer Protocol Secure) zu einem Server herzustellen. Dazu werden SSL-Bibliotheken eingesetzt. Diese Möglichkeit gibt es auch zur verschlüsselten Datenübertragung zwischen Servern. So können alle gängigen Mailserver eine leitungsverschlüsselte Übertragung zu einem anderen Mailserver aufbauen. Falls ein Dritter die übertragenen Daten speichert, könnte er, wenn ihm später die (geheimen) Schlüssel bekannt werden, die Daten nachträglich entschlüsseln. Um diesem Angriff zu verhindern, wurde Perfect Forward Secrecy (PFS) entwickelt (Schlüsselaustausch via Diffie-Hellman). Dabei wird jede einzelne Datenübertragung mit einem eigenen geheimen Schlüssel verschlüsselt, der nicht rekonstruierbar ist.

Die HZD ist Internet-Provider für die Hessische Landesverwaltung und hat ihre externe E-Mail-Übertragung ebenfalls auf Verschlüsselung umgestellt. E-Mails von Landesmitarbeiterinnen und -mitarbeitern, die in das Internet geschickt oder aus dem Internet empfangen werden, werden seit dem 16. April 2014 verschlüsselt übertragen. Voraussetzung für die verschlüsselte Übertragung nach außen ist jedoch, dass die beteiligten Internet-Provider Verschlüsselung unterstützen. Wie schon beschrieben, liegen die

E-Mails im Unterschied zu einer Ende-zu-Ende-Verschlüsselung auf den Servern im Klartext vor.

Aktueller Stand der Technik ist bei Webservern mindestens TLS 1.0 und bei Mail-Servern StartTLS, beides mit dem o. g. PFS-Verfahren.

3.2.1.2.2 Sicherheitslücken

3.2.1.2.2.1 Heartbleed

Anfang April 2013 wurde eine schwerwiegende Sicherheitslücke in der OpenSSL-Bibliothek – die breite Anwendung bei der Implementierung des TLS-Protokolls findet – unter dem Namen Heartbleed öffentlich. Ein Programmierfehler in der Bibliothek versetzt Angreifer in die Lage, Daten aus dem Speicher eines Servers auszulesen. Die Sicherheitslücke befindet sich in einer Hintergrundfunktion, welche regelmäßig Daten hin und her schickt, um zu prüfen, ob beide Kommunikationspartner noch online sind. Diese Funktionalität nennt sich Herzschlag (Heartbeat). Deshalb wurde die Sicherheitslücke von den Entdeckern Heartbleed genannt, weil die Informationen sozusagen ausbluten. Angreifer können betroffene Server nicht nur so beeinflussen, dass die Herzschlag-Nachricht übermittelt wird, sondern auch andere gespeicherte Informationen, bspw. Passwörter oder E-Mail-Inhalte. Dazu können auch die geheimen Schlüssel eines Server-Zertifikats gehören, so dass die gesamte Verschlüsselung zwischen den Kommunikationspartnern kompromittiert wäre. Außerdem können Angreifer das Sitzungs-Cookie stehlen und damit dann Accounts des Anwenders unter Kontrolle bringen (Session Hijacking). In einer Meldung wurde der Krypto-Guru Bruce Schneier zitiert, der den Fehler als „Katastrophe“ einstuft: „Auf einer Skala von 0 bis 10 ist das eine 11“.

Betreiber von Servern mussten dringend überprüfen, ob sie eine verwundbare OpenSSL-Version einsetzen, und auf eine aktuelle Version updaten. Wenn sie bedroht waren, mussten sicherheitshalber alle Zertifikate erneuert werden. Kurz nach dem Bekanntwerden der Heartbleed-Schwachstelle hatte ein Sicherheitsunternehmen 28 Millionen Computer im öffentlichen Netz gescannt und herausgefunden, dass von denen, die auf Port 443 antworten, also SSL resp. TLS anboten, über 600.000 verwundbar waren. Einen Monat nach Heartbleed hatten die Sicherheitsforscher den Versuch wiederholt und fanden über 300.000 verwundbare Systeme. Bei einem erneuten Scan Mitte des Jahres mussten sie feststellen, dass sich an dieser

Zahl kaum etwas geändert hatte. Das deutet darauf hin, dass Serverbetreiber entweder direkt im Anschluss an das Bekanntwerden einer Lücke patchen oder gar nicht. Im August erreichten den HDSB Eingaben von Bürgern, die Server meldeten, die für die Heartbleed-Sicherheitslücke anfällig waren, obwohl diese schon zu diesem Zeitpunkt Monate lang bekannt war.

Im Testlabor des HDSB konnten die Angaben der Petenten verifiziert werden. Daraufhin wurden die verantwortlichen Stellen in unserem Zuständigkeitsbereich aufgefordert diese Sicherheitslücke zu schließen.

Nach § 9 und dessen Anlage zu Satz 1 BDSG müssen Unternehmen und Behörden technische und organisatorische Maßnahmen treffen, insbesondere um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen oder kopiert werden können. D. h., es müssen Verschlüsselungsverfahren eingesetzt werden, die dem Stand der Technik entsprechen.

Die verantwortlichen Stellen reagierten in der Regel zeitnah, die Sicherheitslücke wurde von allen beseitigt.

3.2.1.2.2.2
Poodle

Im Oktober wurde eine Angriffsmöglichkeit auf das Protokoll SSLv3 unter dem Namen Padding Oracle On Downgraded Legacy Encryption (Poodle) bekannt. Wird dieses Protokoll verwendet, können Angreifer die verschlüsselte Verbindung knacken und bspw. das auch bei Heartbleed mögliche Session-Cookie Hijacking durchführen. Das Protokoll ist schon 15 Jahre alt und längst veraltet, wurde aber zu diesem Zeitpunkt Clients von nahezu allen Servern im Internet als sogenannte Fall-Back-Lösung angeboten. D. h., zum Zwecke der Abwärtskompatibilität bieten Server den anfragenden Clients ältere Protokolle an. Sonst könnten veraltete Browser verschlüsselte Webangebote nicht nutzen.

Der einzige Browser mit einer nennenswerten Verbreitung, welcher das nachfolgende TLS 1.0 nicht unterstützt, ist der Microsoft Internet Explorer 6. Dieser ist aber schon so veraltet und für weitere Sicherheitslücken anfällig, dass er auch für das Surfen auf unverschlüsselten Seiten nicht zu empfehlen ist. Das Abschalten von SSLv3 dürfte also zu keinen Problemen oder Beschwerden führen. Mittlerweile wird geraten, nur noch TLS in der Version 1.1 und höher zuzulassen.

Wie bei den Prüfungen zu den Heartbleed-Eingaben bestätigte sich mir in der Praxis o. g. Vermutung, dass Serverbetreiber entweder direkt im An-

schluss an das Bekanntwerden einer Lücke patchen oder gar nicht. Deshalb habe ich im Testlabor des HDSB eine dreistellige Anzahl von Servern von Unternehmen und Gemeinden getestet bzgl. ihrer SSL-Sicherheitslücken. Das Ergebnis war wie beschrieben.

3.2.2
Orientierungshilfe „Cloud Computing“

Die Orientierungshilfe „Cloud Computing“ der Datenschutzbeauftragten des Bundes und der Länder ist aufgrund der aktuellen Geschehnisse insbesondere der NSA-Affäre unter Federführung meines Hauses überarbeitet worden. Sie betrifft neben technischen auch rechtliche Aspekte.

Die Probleme des Cloud Computing wurden schon mehrfach in meinen früheren Tätigkeitsberichten angesprochen. Sie sind nicht weniger geworden und standen nach wie vor im Zentrum der Beratungen der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises. Ergebnis dieser Beratungen war im Jahr 2011 eine Orientierungshilfe, die freilich nur einen ersten Versuch darstellte. Seit Veröffentlichung dieser Orientierungshilfe vor drei Jahren hat sich das Cloud Computing immer weiter durchgesetzt. Dadurch hat aber auch die datenschutzrechtliche Relevanz von Cloud Computing zugenommen. Cloud-Produkte prägen inzwischen den Alltag aller Menschen, die moderne IT benutzen. Da Wolken grundsätzlich grenzenlos sind, kann das Cloud Computing bei internationalen Konflikten wie bei der einleitend erwähnten NSA-Affäre besondere Brisanz erlangen. Diese Entwicklung hat eine Überarbeitung der Orientierungshilfe erforderlich gemacht, die unter Federführung meines Hauses erfolgte.

Die aktualisierte Orientierungshilfe richtet sich weiterhin an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern.

Neben dem bereits genannten Adressatenkreis sind auch sowohl normale Nutzer als auch kleine Unternehmen angesprochen, die zum Beispiel aktuellere Standardsoftware wie Textverarbeitung, Tabellenkalkulation, Mailprogramme etc. nutzen und dabei auf Cloud-Services zurückgreifen, möglicherweise sogar, ohne sich dessen bewusst zu sein.

Die in der neugefassten Orientierungshilfe dargestellten Anforderungen beziehen sich allerdings nur auf das für die nicht-öffentlichen Stellen und die Bundesverwaltung geltende BDSG. Inwieweit Landesdatenschutzgesetze

oder bestehende bereichsspezifische Regelungen davon abweichende Anforderungen festlegen, ist im Einzelfall sorgfältig zu prüfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die überarbeitete Orientierungshilfe zustimmend zur Kenntnis genommen. Die aktuelle Fassung ist auf meiner Homepage einsehbar (https://www.datenschutz.hessen.de/ft-oh_technik.htm#entry4272).

In den nachfolgenden Absätzen wird der Aufbau der Orientierungshilfe noch einmal kurz erläutert und auf die Unterschiede zur ersten Version eingegangen:

Kapitel 1 führt in das Thema ein und wurde inhaltlich seit der ersten Version nicht verändert.

In **Kapitel 2** werden rund um das Cloud Computing die wichtigsten Begriffe erläutert. Da in der Praxis nach wie vor keine einheitliche Terminologie besteht, haben sich die Definitionen wie bereits in der ersten Version an den Ausführungen des BSI und des Fraunhoferinstitutes für Offene Kommunikationssysteme orientiert. Die Beschreibungen für Cloud-Anwender und Cloud-Anbieter, die Basisinfrastrukturen Public Cloud, Private Cloud und Community Cloud und die Betriebsmodelle SaaS, PaaP und IaaS werden der rechtlichen Bewertung in der Orientierungshilfe zugrunde gelegt.

Kapitel 3 der Orientierungshilfe setzt sich mit den datenschutzrechtlichen Aspekten des Cloud Computing, insbesondere mit der Verantwortlichkeit des Cloud-Anwenders, der Kontrolle des Cloud-Anbieters und den Betroffenenrechten auseinander. Diese Passagen/Abschnitte wurden inhaltlich überarbeitet. Neu aufgenommen wurden die Themen „Unrechtmäßige Kenntniserlangung von Daten“ und „Verarbeitung von verschlüsselten Daten“. Weiterhin wird der grenzüberschreitende Datenverkehr (innereuropäischer (Kap.: 3.1.1) und außereuropäischer Raum (Kap.: 3.1.2)) beleuchtet. Ein eigenes Kapitel 3.1.3 widmet sich jetzt den neueren Entwicklungen und deren Bewertung. Die Orientierungshilfe gibt klare Empfehlungen zum datenschutzgerechten Einsatz.

Kapitel 4 wurde neu strukturiert und überarbeitet. Es beschäftigt sich mit den technischen und organisatorischen Aspekten.

Cloud-Computing-Systeme der Cloud-Anbieter unterliegen infrastrukturellen Rahmenbedingungen: Die Schutzziele der IT (Verfügbarkeit, Vertraulichkeit, Integrität) und die Schutzziele des Datenschutzes (Datensparsamkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit) müssen gewährleistet werden. Neu aufgenommen wurden bei der Betrachtung die Schutzziele des Datenschutzes Datensparsamkeit, Intervenierbarkeit und Nichtverkettbarkeit (Kapitel 4.1.1). Die Umsetzung aller Schutzziele ist durch

technische und organisatorische Maßnahmen abzusichern. Cloud-Computing-Systeme unterliegen ebenso wie klassische Computersysteme sowohl klassischen als auch typisch cloud-spezifischen Risiken. Kapitel 4.1.2 widmet sich den klassischen Risiken. In Kapitel 4.1.3 werden die grundsätzlichen cloud-spezifischen Risiken, die ein Erreichen der Schutzziele erschweren, näher erläutert.

In dem nachfolgenden Kapitel 4.2 Cloud-Betriebsmodelle werden anhand der beschriebenen Schutzziele – nun erweitert um die Datensparsamkeit, Intervenierbarkeit und Nichtverkettbarkeit – für die verschiedenen Betriebsmodelle IaaS, PaaS, SaaS die Risiken spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

Kapitel 4.3 Zertifizierungen ist neu.

Kapitel 5 zieht ein Fazit. Der erste Teil ist im Wesentlichen gleich geblieben. Der zweite Teil ist neu hinzugekommen und beinhaltet eine Zusammenfassung der Neubewertung.

Kapitel 5 Teil 1

Cloud Computing steht für vielfältige Möglichkeiten, Dienstleistungen zur Datenverarbeitung unter Verwendung des Internets oder anderer Wide Area Networks wie Konzernnetze oder die Landesnetze der Verwaltungen in Anspruch zu nehmen. Ob Public, Private, Community oder Hybrid Clouds, ob SaaS, PaaP oder IaaS: Allen Varianten gemein ist, dass die Anwender Leistungen von Anbietern in Anspruch nehmen, die über das jeweilige Netz erreicht werden können, die wegen ihrer Skalierbarkeit flexibel an den jeweils aktuellen Bedarf angepasst werden können und nach Verbrauch bezahlt werden. Bei allen Varianten unterschiedlich sind jedoch der Umfang und die Art der Dienstleistung, die Bestimmt- oder Unbestimmtheit der Verarbeitungsorte, die Einflussmöglichkeiten der Anwender auf die örtlichen, infrastrukturellen und qualitativen Rahmenbedingungen der Verarbeitung. Unterschiedlich sind auch die datenschutzrechtlichen und informationssicherheitstechnischen Anforderungen.

Die wirtschaftlichen Vorteile des Cloud Computing für die Anwender sind nicht zu übersehen. Die starke Reduktion der selbst noch vorzuhaltenden Infrastruktur, die Verringerung des Bedarfs an eigenem IT-Fachpersonal, die Vermeidung von Risiken der Über- und Unterkapazitäten und die bessere Übersichtlichkeit der Kosten der Datenverarbeitung sind für Unternehmen und Behörden gute Gründe, die Beauftragung von Cloud-Computing-Anbietern in Erwägung zu ziehen.

Problematisch ist es jedoch, die Compliance-Anforderungen an die Datenverarbeitung der Unternehmen und Behörden, zu denen Datenschutz und Informationssicherheit, aber auch die Kontrollierbarkeit, Transparenz und Beeinflussbarkeit gehören, unter den Rahmenbedingungen des Cloud Computing, insbesondere in der Public Cloud, zu erfüllen. Es muss verhindert werden, dass die Fähigkeit der Organisationen, allen voran ihrer Leitungen, die Verantwortung für die eigene Datenverarbeitung noch tragen zu können, durch das Cloud Computing untergraben wird.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Anwender klare Entscheidungskriterien bei der Wahl zwischen den Anbietern haben, aber auch, ob Cloud Computing überhaupt in Frage kommt;
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ kann;
- die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender;
- die Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der o. g. Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.

Kapitel 5 Teil 2

Zur Gewährleistung einer rechtmäßigen Weitergabe personenbezogener Daten an einen Cloud-Anbieter, der außerhalb der EU/des EWR seinen Sitz hat, bedarf es in erster Linie der Verwendung von Standardvertragsklauseln oder BCRs, wobei der Beschreibung und Umsetzung technisch-organisatorischer Sicherheitsmaßnahmen eine besondere Bedeutung zukommt. Rechtsgrundlage für die Datenweitergabe an einen Cloud-Anbieter kann in diesem Zusammenhang § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein.

28 Abs. 1 Satz 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

1. *...*
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, ...*

Eine Rechtsgrundlage für die Weitergabe besonderer personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG wird dabei regelmäßig nicht bestehen, da die Anforderungen nach § 28 Abs. 6 bis 9 BDSG nicht erfüllt sind.

Soweit öffentliche Stellen Cloud-Services in Drittstaaten in Anspruch nehmen, ist eine besonders sorgfältige Prüfung der Rechtsgrundlage geboten. Einen dem § 28 Abs. 1 Satz 1 Nr. 2 BDSG entsprechenden Erlaubnistatbestand gibt es im HDSG nicht.

Da insbesondere außereuropäische Behörden nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden, muss eine Neubewertung vorgenommen werden. Bevor nicht der unbeschränkte Zugriff ausländischer Nachrichtendienste auf personenbezogene Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird, behalten sich die Aufsichtsbehörden für den Datenschutz vor, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen, und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind.

4. Datenschutz im öffentlichen Bereich

4.1
Hessen

4.1.1
Hessen Querschnitt

4.1.1.1
Funktionaler Stellenbegriff – Datenübermittlung zwischen verschiedenen Ämtern eines Landkreises

Zwischen den einzelnen Fachdiensten einer Kreisverwaltung dürfen personenbezogene Daten grundsätzlich nur aufgrund einer gesetzlichen Befugnis übermittelt werden. Der interne Datenaustausch („auf dem kurzen Dienstweg“) bedarf daher stets einer Einzelfallprüfung.

4.1.1.1.1
Der Anlass

Ausgangspunkt war eine Eingabe eines Bürgers betreffend die Weitergabe von personenbezogenen Daten innerhalb einer Abteilung der Kreisverwaltung eines hessischen Landkreises. Von der Abteilung der Kreisverwaltung wurde mir mitgeteilt, dass gegen eine derartige Weitergabe von Informationen schon deshalb keine Bedenken bestehen, weil sich das Ganze innerhalb einer Abteilung abspiele. Da diese Argumentation nach meiner Auffassung unzutreffend ist, möchte ich den Fall nochmals zur Klarstellung nutzen.

Im vorliegenden Fall gliedert sich die betreffende Abteilung in fünf Fachdienste, unter anderem das „Ausländer- und Personenstandswesen“ sowie das „personenbezogene Verkehrswesen“. Der Fachdienst „Ausländer- und Personenstandswesen“ hatte aufgrund einer ärztlichen Bescheinigung in einem ausländerrechtlichen Verfahren Kenntnis darüber erlangt, dass ein deutscher Fahrerlaubnisbesitzer unter gesundheitlichen Beeinträchtigungen leidet, die möglicherweise der sicheren Teilnahme am Straßenverkehr entgegenstehen. Die betreffenden Informationen wurden auf Verfügung des Abteilungsleiters an den Fachdienst „personenbezogenes Verkehrswesen“ weitergeleitet mit der Bitte, die gesundheitliche Eignung des Fahrerlaubnisbesitzers zum Führen von Kraftfahrzeugen zu überprüfen. Gegen diese Datenweitergabe wandte sich der Petent.

4.1.1.1.2
Datenschutzrechtliche Bewertung

Aus datenschutzrechtlicher Sicht ist zu unterscheiden, ob der Fachdienst, der die Informationen erhält, reiner „Empfänger“ oder „Dritter“ ist. Ist der Fachdienst als Dritter anzusehen, liegt eine Datenübermittlung im Sinne des § 2 Abs. 2 Satz 2 Nr. 3 HDSG und nicht lediglich eine Weitergabe vor, und es gelten die gesetzlichen Übermittlungsschranken.

§ 2 Abs. 2 Satz 2 Nr. 3 HDSG

Im Sinne der nachfolgenden Vorschriften ist

…

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft, …

Wer „Dritter“ ist, regelt § 2 Abs. 5 HDSG:

§ 2 Abs. 5 HDSG

Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen oder Stellen, die innerhalb des Geltungsbereichs der EG-Datenschutzrichtlinie Daten im Auftrag verarbeiten.

Nach dem dieser Vorschrift zugrunde liegenden funktionalen Behördenbegriff ist jeder organisatorische Teilbereich einer Organisationseinheit, der eine eigene Aufgabe bzw. Funktion ausfüllt, „Dritter“. Dies gilt deshalb auch für die einzelnen Fachdienste im Verhältnis zueinander. Der Fachdienst „Ausländer- und Personenstandswesen“ und der Fachdienst „personenbezogenes Verkehrswesen“ nehmen unterschiedliche Aufgaben wahr und verarbeiten personenbezogene Daten zu unterschiedlichen Zwecken. Sie sind damit als eigenständige datenverarbeitende Stellen zu betrachten und eine Datenweitergabe von einem Fachdienst zum anderen Fachdienst unterliegt den Übermittlungsvorschriften (funktionaler Stellenbegriff), selbst wenn sie Teile einer verwaltungsrechtlichen Einheit (Kreisverwaltung) sind.

Für die Ausländerbehörde besteht vorliegend keine spezialgesetzliche Übermittlungsbefugnis im Aufenthaltsgesetz, so dass auf das allgemeine Datenschutzrecht zurückzugreifen ist. Nach § 13 Abs. 2 Satz 1 i. V. m. § 12 Abs. 2 Nr. 3 HDSG ist eine zweckändernde Datenverarbeitung unter bestimmten Voraussetzungen zulässig.

§ 13 Abs. 2 Satz 1 HDSG

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

§ 12 Abs. 2 Nr. 3 HDSG

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

…

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

Daten, die Zweifel an der gesundheitlichen Eignung zum Führen von Kraftfahrzeugen begründen, können auf dieser Grundlage grundsätzlich übermittelt werden, wenn die gesundheitliche Beeinträchtigung so erheblich ist, dass die in § 12 genannten Gefahren oder Nachteile zu befürchten sind. Da dies nach Aktenlage vorliegend der Fall war, war die zweckändernde Datenübermittlung an die Fahrerlaubnisstelle nicht zu beanstanden. Anders hätte die datenschutzrechtliche Bewertung beispielsweise ausfallen können, wenn die Gesundheitsbeeinträchtigung für das Führen eines Fahrzeugs irrelevant gewesen wäre.

4.1.1.2
Auftragsdatenverarbeitung – Kontrollrechte des Hessischen Datenschutzbeauftragten

Auftragnehmer, die für eine öffentliche hessische Stelle Datenverarbeitungsdienstleistungen erbringen, müssen sich der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwerfen, sofern sie nicht ohnehin bereits seiner Kontrolle unterfallen.

Die Stadt Frankfurt – Energiereferat – hat mit einer privaten Firma mit Sitz in Köln einen Hostingvertrag abgeschlossen. Ausweislich des Vertragstextes ist Gegenstand des Auftrags nicht die originäre Nutzung oder Verarbeitung von personenbezogenen Daten durch die Auftragnehmerin. Aber im Zuge der Leistungserbringung der Auftragnehmerin als zentraler IT-Dienstleister im Bereich des Hostings, des Supports bzw. der Administration von Server-Systemen der Auftraggeberin Stadt Frankfurt kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.

Damit handelt es sich bei der Dienstleistung der beauftragten Firma rechtlich um Datenverarbeitung im Auftrag, die im Auftrag der Stadt Frankfurt für

diese erbracht wird. Nach § 4 HDSG gilt für den Auftragnehmer einer öffentlichen hessischen Stelle das gleiche Datenschutzrecht wie für den Auftraggeber, d. h., auch der private Dienstleister hat die Vorschriften des HDSG zu befolgen, soweit er als Auftragnehmer für die Stadt Frankfurt tätig wird.

§ 4 Abs. 3 HDSG

Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

Demnach ist die Auftraggeberin Stadt Frankfurt gesetzlich verpflichtet, vertraglich sicherzustellen, dass die Auftragnehmerin die Bestimmungen des HDSG befolgt und diese sich zudem der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwirft, soweit sie für die Stadt Frankfurt tätig wird.

Das Energiereferat der Stadt Frankfurt ist im Vorfeld des Vertragsabschlusses über dieses rechtliche Erfordernis durch den behördlichen Datenschutzbeauftragten der Stadt umfassend informiert worden. Er hat sowohl Gespräche mit Mitarbeitern des Energiereferats als auch Schriftverkehr mit dem Referat geführt. Der Dienstleister aus Köln war allerdings nicht bereit, einen Vertrag mit der geforderten Unterwerfungserklärung zu unterzeichnen. Der behördliche Datenschutzbeauftragte hat daraufhin das Energiereferat belehrt, dass unter diesen Umständen ein Vertragsabschluss nicht möglich ist. Gleichwohl hat die Stadt Frankfurt mit diesem Dienstleister unter Missachtung der Rechtslage einen Vertrag abgeschlossen. Auf meine Aufforderung, diesen Vertrag nachzubessern, hat die Stadt vorgetragen, dass man sich bei den Anforderungen im „Massenmarkt“ bewege. Man nutze ein Server- und Hosting-Produkt, welches in dieser Form von den Anbietern standardisiert angeboten werde. Eine Individualisierung der Vertragsbedingungen sei für diese Produktoption nicht vorgesehen. Eine Individualisierung würde erhebliche Kosten verursachen, eine Anpassung des Vertrages an das HDSG sei aus wirtschaftlichen Gründen deshalb nicht darstellbar.

Da ein an die Rechtslage angepasster Vertrag erheblich teurer sei, habe man aus Angemessenheitserwägungen auf die Unterwerfungserklärung verzichtet.

Ich sah mich aus diesem Grund veranlasst, das Vorgehen der Stadt Frankfurt förmlich nach § 27 HDSG zu beanstanden und den Hessischen Innen-

minister als zuständige Kommunalaufsicht darüber zu informieren. Die Stadt Frankfurt hat aus haushaltsrechtlichen Erwägungen trotz meiner Beanstandung darauf bestanden, an dem abgeschlossenen Vertrag festzuhalten. Auch darüber habe ich den Hessischen Innenminister informiert.

Das Innenministerium hat daraufhin die Stadt Frankfurt zunächst darüber belehrt, dass im Falle von Beanstandungen durch den Hessischen Datenschutzbeauftragten die beanstandete Stelle verpflichtet ist, ihre dem Hessischen Datenschutzbeauftragten abgegebene Stellungnahme gemäß § 27 Abs. 4 S. 2 HDSG auch der Kommunalaufsicht zuzuleiten. Dies hatte die Stadt Frankfurt versäumt.

Im Übrigen hat das Innenministerium geäußert, dass nicht erkennbar sei, warum die Anpassung eines Vertrages an die im HDSG geforderte Unterwerfung unter die Kontrolle des Hessischen Datenschutzbeauftragten bei den Dienstleistern einen besonderen Aufwand verursachen soll, der die angeführten Preise rechtfertigen soll. Es hat insoweit eine Neubewertung dahingehend gefordert, welcher erhöhte Aufwand für den Dienstleister wegen einer zusätzlichen und auf den Umfang eines einzigen Auftrags beschränkten Kontrolle durch den Hessischen Datenschutzbeauftragten in der Praxis überhaupt entsteht.

Infolgedessen ist die Stadt Frankfurt mit der Auftragnehmerin noch einmal in Kontakt getreten. Diese hat daraufhin die Bereitschaft signalisiert, den Vertrag an die Regelungen des HDSG anzupassen. Inzwischen liegt mir ein Vertragsentwurf mit der geforderten Unterwerfungserklärung vor.

4.1.1.3
Abgrenzung von öffentlicher Auslegung, öffentlicher Bekanntmachung und Internetöffentlichkeit

Daten, die aufgrund einer Rechtsgrundlage entweder öffentlich bekannt gemacht oder öffentlich ausgelegt werden und damit jedem interessierten Bürger zur Einsichtnahme zugänglich sind, dürfen ohne ausdrückliche Rechtsgrundlage nicht automatisch auch im Internet veröffentlicht werden.

Zur Information der Allgemeinheit sehen einige Gesetze vor, dass die Bürgerinnen und Bürger im Wege der öffentlichen Bekanntmachung über Beschlüsse der Verwaltung informiert werden. Daneben gibt es auch die Information über den Weg der öffentlichen Auslegung, die regelmäßig nur über einen bestimmten beschränkten Zeitraum stattfindet. Hier stellt sich für die Verwaltungen regelmäßig die Frage, ob derartig öffentlich gemachte Informationen auch im Internet veröffentlicht werden dürfen.

Für öffentliche Bekanntmachungen der Gemeinden hat der hessische Gesetzgeber diese Frage durch § 7 der Hessischen Gemeindeordnung (HGO) beantwortet.

§ 7 Abs. 1 HGO

Öffentliche Bekanntmachungen der Gemeinden erfolgen in einer örtlich verbreiteten, mindestens einmal wöchentlich erscheinenden Zeitung, in einem Amtsblatt oder im Internet.

4.1.1.3.1
Stellenplan im Internet

Aus einer hessischen Kommune wurde die Frage an mich herangetragen, ob der Stellenplan einer Kommune im Internet veröffentlicht werden dürfe.

Gemäß § 97 Abs. 5 HGO ist die Haushaltssatzung öffentlich bekannt zu machen. Damit darf die Haushaltssatzung nach § 7 HGO auch im Internet veröffentlicht werden. Der Haushaltsplan, zu dem auch der Stellenplan gehört, ist hingegen nur an 7 Tagen öffentlich auszulegen. Für die öffentliche Auslegung findet sich in der HGO aber keine dem § 7 Abs. 1 entsprechende Vorschrift, nach der auch diese im Internet zulässig wäre. Mindestens für die Teile des Haushaltsplanes, die (wie der Stellenplan) personenbeziehbar sind, mangelt es daher an der erforderlichen Rechtsgrundlage für eine Veröffentlichung im Internet.

Dass der Gesetzgeber hierfür keine dem § 7 Abs. 1 HGO entsprechende Rechtsgrundlage geschaffen hat, ist aus meiner Sicht rechtlich geboten. Wenn Unterlagen für einen begrenzten Zeitraum einer interessierten Öffentlichkeit zugänglich gemacht werden sollen, dann sollen sie gerade nicht in aller Welt frei verfügbar sein. Sie stehen den Bürgern in der Kommune, in der Regel in Räumen der Verwaltung, für z. B. 7 Tage zur Verfügung und sind dann wieder der Öffentlichkeit entzogen. Das Internet kennt kein „Recht auf Vergessen“. Wenn demnach von vorneherein klar ist, dass nur über einen kurzen Zeitraum der Öffentlichkeit die Gelegenheit der Kenntnisnahme bestimmter Entscheidungen/Pläne etc. gegeben werden soll, dann kann für eine Internetveröffentlichung kein Raum sein. Dies würde den Gedanken der begrenzten Öffentlichkeit konterkarieren.

4.1.1.3.2
Vorschlagsliste zur Schöffenwahl im Internet

Durch eine weitere Eingabe bin ich auf einen weiteren Fall der begrenzten Öffentlichkeit aufmerksam gemacht worden.

Eine Kommune veröffentlichte auf ihrer Homepage im Bereich Bürgerservice die Vorschlagsliste für die Schöffenwahl 2014 bis 2018. § 36 Abs. 3 Gerichtsverfassungsgesetz (GVG) schreibt vor, dass die Vorschlagsliste in der Gemeinde eine Woche lang zu jedermanns Einsicht auszulegen ist. Von einer Internetveröffentlichung ist hier ebenfalls nicht die Rede. Da die Vorschlagsliste auch noch deutlich über den Zeitraum der Wochenfrist im Internet zu finden war, war diese Veröffentlichung m. E. gleich in doppelter Hinsicht unzulässig. Sie erfolgte ohne Rechtsgrundlage und über die zulässige Frist hinaus. Ich habe die Kommune aufgefordert, die Schöffenliste aus dem Internet zu entfernen. Dies ist geschehen.

4.1.2
Justiz, Polizei und Verfassungsschutz

4.1.2.1
Einsatz von BodyCams bei der hessischen Polizei

Der punktuelle Einsatz von sog. „BodyCams“ im Rahmen von Personenkontrollen ist grundsätzlich möglich. Gegen eine Ausweitung auch auf Tonaufnahmen in diesem Kontext bestehen erhebliche Bedenken.

Seit Mai 2013 wurden – zunächst in Frankfurt im Bereich Alt Sachsenhausen und im Anschluss zusätzlich im Bereich der Zeil sowie ab Ende 2013 auch im Zuständigkeitsbereich der Polizeipräsidien Südosthessen und Westhessen – im Rahmen eines Pilotprojektes sogenannte BodyCams eingesetzt. Die ursprünglichen Rahmenbedingungen des Projekts waren mit mir abgestimmt.

Bei den BodyCams handelt es sich um kleine Videokameras, die am Körper getragen werden. Für das Modellprojekt war eine Kamera ausgesucht worden, die auf der Schulter getragen wird und über eine Fernbedienung gesteuert werden kann. Die Beamten, die die Kamera führen, tragen eine spezielle Weste, die die Videoüberwachung kenntlich macht.

Bei jedem Einsatz von Videotechnik handelt es sich um einen Eingriff in das Recht auf informationelle Selbstbestimmung. Dafür ist eine gesetzliche Grundlage erforderlich. Diese ergibt sich in diesem Zusammenhang aus § 14 Abs. 6 HSOG.

§ 14 Abs. 6 HSOG

Die Polizeibehörden können an öffentlich zugänglichen Orten eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, mittels Bildübertragung offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum

Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Dabei können personenbezogene Daten auch über dritte Personen erhoben werden, soweit dies unerlässlich ist, um die Maßnahme nach Satz 1 durchführen zu können. Sind die Daten für Zwecke der Eigensicherung oder der Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich zu löschen.

Ursprünglich war diese Norm 2005 geschaffen worden, um Beamte bei Kontrollen – insbesondere im Straßenverkehr – besser vor Angriffen zu schützen. Vorgesehen war daher die Ausstattung von Streifenwagen mit entsprechenden Kameras. Da der Wortlaut der Regelung an die Kontrollsituation – Feststellung der Identität – und nicht an die Art des Einsatzes anknüpft, ist auch die Verwendung einer BodyCam auf dieser Grundlage grundsätzlich möglich.

Für einen zulässigen Einsatz sind die folgenden Rahmenbedingungen maßgelblich:

Der Einsatz einer BodyCam muss in dem vorgesehenen räumlichen Bereich erforderlich sein und er muss darüber hinaus in der konkreten Einsatzsituation erforderlich sein (doppelte Erforderlichkeit). Mit diesen Vorgaben halte ich die Planung des Innenministers, alle Präsidien mit dieser Technik auszustatten, grundsätzlich für zulässig. Jedoch muss in dem jeweiligen Präsidium ein Konzept erstellt werden, in welchen Bereichen bzw. bei welchen Situationen die Kamera zum Einsatz kommen darf. Während des Einsatzes muss dann vor Ort entschieden werden, ob die konkreten Voraussetzungen – eine Gefahr für Leib oder Leben der Beamten oder Dritter – gegeben sind. Erst dann kann die Beobachtung und Aufzeichnung der BodyCam aktiviert werden.

Das bedeutet für die Praxis zunächst, dass die Kamera nicht auf dem gesamten Streifengang eingeschaltet sein darf. Da es sich nach den gesetzlichen Voraussetzungen um eine offene Überwachung handelt, muss nach meiner Einschätzung nicht nur der Beginn der Aufnahme mitgeteilt werden, sondern der Betrieb der laufenden Kamera muss für das Umfeld erkennbar sein. Zudem muss vor der Aktivierung auf diese hingewiesen werden. Die Kennzeichnung der Beamten mit der Weste allein ist nicht ausreichend. Auch sollte an der Kamera erkennbar sein, dass die Aufzeichnung erfolgt, etwa durch eine Lampe.

Zu den von mir geforderten Rahmenbedingungen des Projektes gehören auch Vorgaben zum weiteren Umgang mit in der Kamera gespeicherten Sequenzen. So sind unmittelbar nach Rückkehr in die Dienststelle die Aufnahmen zu sichten und alle Sequenzen zu löschen, an die sich nicht weitere Maßnahmen anschließen können. Eine denkbare Maßnahme kann zum ei-

nen die Nutzung als Beweismittel sein, wenn sich aus der Kontrollsituation Strafverfahren ergeben. Zulässig ist aber auch eine Speicherung der Aufnahmen, um den konkreten Einsatz zu dokumentieren, weil Beschwerden oder Anzeigen von Betroffenen oder Dritten nicht auszuschließen sind. Die Selektion der Aufnahmen erfolgt durch die Dienstgruppenleiter, nicht durch die vor Ort eingesetzten Beamten selbst. Die zu sichernden Aufnahmen werden mittels eines USB-Anschlusses auf einen Einzelplatzrechner übertragen.

Soweit es zu einem Strafverfahren kommt, dienen die Aufnahmen als Beweismittel. Die entsprechende Sequenz wird dazu auf einen Datenträger übertragen, der zum entsprechenden Verfahren asserviert wird. Die Aufbewahrungsdauer richtet sich dann nach den Regeln der StPO. Andere Sequenzen können bis zu 6 Monate aufbewahrt werden. Dieser relativ langen Frist habe ich zugestimmt, da damit die Aufnahmen auch zur Verfügung stehen, wenn sich eine Notwendigkeit der abschließenden Bewertung eines konkreten Einsatzes nicht sofort ergibt. Nach polizeilicher Erfahrung kann es einige Zeit dauern, bis Betroffene Polizeibeamte anzeigen. Dies geschieht zum Teil auch erst als Reaktion auf ein Ermittlungsverfahren.

Für den flächendeckenden Einsatz der BodyCams wurde durch das Landespolizeipräsidium eine Handlungsempfehlung erstellt.

In der vorbereitenden Diskussion habe ich auf Folgendes hingewiesen:

Derzeit stützt sich der Einsatz von BodyCams wie dargelegt auf § 14 Abs. 6 HSOG. Dessen strenge Rahmenbedingungen sind daher einzuhalten.

Die Maßnahme der Videoüberwachung ist eine präventive Maßnahme, das Beobachten und ggf. Aufzeichnen soll Gefährdungen verhindern. Auch wenn im Einzelfall durch die Aufzeichnungen das korrekte Geschehen vor Ort nachgewiesen werden kann, ist die generelle Dokumentation eines Einsatzes auf dieser Rechtsgrundlage nicht möglich. Zudem ist die Maßnahme an eine Identitätsfeststellung geknüpft.

Des Weiteren ist sicherzustellen, dass die Aktivierung der Kamera deutlich für alle erkennbar ist. Nach meiner Einschätzung ist dazu ein verbaler Hinweis des die Kamera tragenden Beamten nicht ausreichend. Dieser kann in der Situation überhört werden, ggf. geraten auch erst später Personen in den Fokus der Kamera, die die Ankündigung nicht wahrnehmen konnten.

Die Kamera darf erst aufnehmen, nachdem vor Ort entschieden wurde, dass eine konkrete Gefährdung besteht. Ein permanentes Aufzeichnen von Kamerabildern in einem Ringspeicher mit dem Ziel, im Falle der Aktivierung der Speicherung auch einen (begrenzten) Zeitraum in der Vergangenheit mit zu sichern (sog. Pre-recording), halte ich auf der gegenwärtigen Rechtsgrundlage für unzulässig.

Die gesetzliche Regelung setzt schon für die Beobachtung mittels einer Videokamera voraus, dass eine konkrete Gefahr für Leib oder Leben besteht. Auch wenn grundsätzlich nach der Rechtsprechung des Bundesverfassungsgerichtes (Urteil des BVerfG vom 23. November 2008, 1 BvR 2074/05) keine Datenerhebung vorliegt, soweit Daten im System sofort verarbeitet und spurenlos gelöscht werden, wenn die Voraussetzungen der Datenerhebung – die mit dem Einsatz der konkreten Technik erfolgen soll – nicht vorliegen, kann damit ein permanentes Aufzeichnen der Kamera nicht gerechtfertigt werden.

Das Mitführen einer Videokamera kann schon das Verhalten der Menschen beeinflussen, die sich im vermeintlichen Fokus befinden. Daher ist auch für jeglichen Einsatz von Videotechnik durch die Polizei eine ausdrückliche Rechtsgrundlage erforderlich. § 14 Abs. 6 HSOG setzt eine konkrete Gefährdung voraus. Diese Vorschrift ist nicht als Grundlage für einen permanenten Einsatz ausgestaltet. Personen auf der Straße müssen nicht damit rechnen, dass sie jederzeit beobachtet werden, zumal sie nicht erkennen können, inwieweit (auch) die Aufzeichnungsfunktion der Kamera aktiviert ist.

Überlegungen aus den Reihen der Polizei, die Einsatzmöglichkeiten der BodyCams zu erweitern, sind daher nach meiner Einschätzung nur realisierbar, wenn dafür eine präzise Rechtsgrundlage geschaffen wird.

Dies gilt auch für die Ankündigung des Innenministers, die Möglichkeiten für Tonaufnahmen zu prüfen. Durch Tonaufnahmen erfolgt ein zusätzlicher Grundrechtseingriff. Dieser betrifft sowohl die unmittelbar zu kontrollierenden Personen als auch Unbeteiligte im Umfeld der Kontrollsituation. Zur Begründung der Überlegungen wird insbesondere auf die Verhinderung bzw. Verfolgung von Beleidigungen der Beamten verwiesen. Soweit es um die Strafverfolgung geht, sind die notwendigen Maßnahmen in der StPO festzulegen. Im Vergleich zu den derzeit möglichen Bildaufnahmen wäre der Anlass für den Eingriff zudem erheblich niedrigschwelliger. Dies ist bei der Abwägung der Grundrechte von Kontrollierten und Kontrollierenden zu berücksichtigen. Bei allem Verständnis für die betroffenen Beamten besteht doch im Unrechtsgehalt ein erheblicher Unterschied zwischen Gefährdungen für Leib und Leben oder Beleidigungen.

Ich habe daher erhebliche Zweifel, ob eine solche Eingriffsnorm unter dem Gesichtspunkt der Verhältnismäßigkeit verfassungsgemäß ausgestaltet werden kann.

4.1.2.2
Verarbeitung der Daten des Landesamtes für Verfassungsschutz durch das Bundesamt

Auch soweit das Bundesamt für Verfassungsschutz anbietet, in seinem Rechenzentrum Datenbanken der Landesämter für Verfassungsschutz zu führen, sind die allgemeinen Regeln etwa zur Auftragsdatenverarbeitung zu beachten.

Grundlage für das Speichern von Daten ist für das Hessische Landesamt § 6 des Gesetzes über das Landesamt für Verfassungsschutz (HVerfSchG).

§ 6 HVerfSchG

(1) Umfang und Dauer der Speicherung personenbezogener Daten sind auf das für die Aufgabenerfüllung des Landesamtes für Verfassungsschutz erforderliche Maß zu beschränken.

(2) Das Landesamt für Verfassungsschutz darf Daten über Minderjährige, die das 14. Lebensjahr nicht vollendet haben, in zu ihrer Person geführten Akten nur speichern, wenn tatsächliche Anhaltspunkte dafür bestehen, dass der Minderjährige eine der in § 3 des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat. In Dateien ist eine Speicherung von Daten Minderjähriger, die das 14. Lebensjahr nicht vollendet haben, nicht zulässig.

(3) In Dateien oder zu ihrer Person geführten Akten gespeicherte Daten über Minderjährige sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse angefallen sind, die eine Fortdauer der Speicherung rechtfertigen.

(4) Personenbezogene Daten, die erhoben worden sind, um zu prüfen, ob Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen, dürfen in Dateien erst gespeichert werden, wenn sich tatsächliche Anhaltspunkte für derartige Bestrebungen oder Tätigkeiten ergeben haben. Bis zu diesem Zeitpunkt dürfen auch keine Akten angelegt werden, die zur Person geführt werden.

(5) Das Landesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und im Übrigen nach von ihm festgesetzten angemessenen Fristen, spätestens jedoch nach fünf Jahren, ob gespeicherte personenbezogene Daten zur Aufgabenerfüllung noch erforderlich sind. Gespeicherte personenbezogene Daten über Bestrebungen nach § 2 Abs. 2 Nr. 1 sind spätestens 10 Jahre, über Bestrebungen nach § 2 Abs. 2 Nr. 3 und 5 sind spätestens 15 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, der Behördenleiter oder sein Vertreter trifft im Einzelfall ausnahmsweise eine andere Entscheidung. Enthalten Sachakten oder Akten zu anderen Personen personenbezogene Daten, die nach Satz 2 zu löschen sind, dürfen sie nicht mehr verwendet werden. Soweit Daten automatisiert verarbeitet oder Akten automatisiert erschlossen werden, ist auf den Ablauf der Fristen nach Satz 1 und 2 hinzuweisen.

In weiten Teilen entspricht die Datei des LfV den Daten, die im Nachrichtendienstlichen Informationssystem (NADIS) gemäß § 6 BVerfSchG beim BfV auf Grund der Verpflichtung zur Zusammenarbeit im Verfassungs-

schutzverbund zu speichern sind. NADIS war ursprünglich nur ein System zum Nachweis der geführten Personen- und Sachakten, wie in § 6 Satz 2 BVerfSchG vorgesehen. Mit der seit 2012 erfolgten Erweiterung des Systems zum Nachrichtendienstlichen Informationssystem und Wissensnetz (NADIS WN) ist es nunmehr möglich, auch Hinweisdaten und Texte zu erfassen, soweit dabei die Voraussetzungen des § 6 Satz 8 BVerfSchG eingehalten werden. Dazu gehört insbesondere, dass die Zugriffsberechtigung auf die Personen zu beschränken ist, die unmittelbar mit der Bearbeitung des jeweiligen Sachzusammenhangs betraut sind.

§ 6 BVerfSchG

Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach § 5 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Die Speicherung personenbezogener Daten ist nur unter den Voraussetzungen der §§ 10 und 11 zulässig. Der Abruf im automatisierten Verfahren durch andere Stellen ist nicht zulässig. Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede Verfassungsschutzbehörde nur für die von ihr eingegebenen Daten; nur sie darf diese Daten verändern, sperren oder löschen. Die eingebende Stelle muss feststellbar sein. Das Bundesamt für Verfassungsschutz trifft für die gemeinsamen Dateien die technischen und organisatorischen Maßnahmen nach § 9 des Bundesdatenschutzgesetzes. Die Führung von Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, ist unter den Voraussetzungen dieses Paragraphen nur zulässig für eng umgrenzte Anwendungsgebiete zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht, von rechtsextremistischen Bestrebungen oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten. Die Zugriffsberechtigung ist auf Personen zu beschränken, die unmittelbar mit Arbeiten in diesem Anwendungsgebiet betraut sind; in der Dateianordnung (§ 14) ist die Erforderlichkeit der Aufnahme von Textzusätzen in der Datei zu begründen.

Das BfV bietet den Ländern seit einiger Zeit an, die Amtsdateien in seinem Rechenzentrum zu verarbeiten. Die Struktur der Datenbank soll dabei der von NADIS WN entsprechen. Durch technische Maßnahmen sei sichergestellt, dass nur Berechtigte Zugriff auf diese Daten haben. Die technische Organisation der Datenverarbeitung und alle Sicherheitsmaßnahmen im Rechenzentrum einschließlich der Administrationsaufgaben bleiben dabei voll in der Verantwortung des BfV. Dieses Angebot soll den Ländern zum einen eine doppelte Erfassung einzelner Datensätze, aber auch nicht unerhebliche Kosten für das Entwickeln und Betreiben der entsprechenden Datenbanken ersparen.

Das BfV beruft sich bei seinem Angebot auf die Möglichkeit der „Amtshilfe“. Für die Zulässigkeit und Ausgestaltung dieses Angebotes beruft es sich auf

§ 1 Abs. 3 BVerfSchG. Aus dieser Vorschrift ergibt sich jedoch lediglich eine allgemeine Pflicht zur Zusammenarbeit, nicht die Befugnis zur Verarbeitung personenbezogener Daten – in welcher Form auch immer –.

§ 1 Abs. 3 BVerfSchG

Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

Grundsätzlich ist eine Datenverarbeitung durch Dritte auch im Rahmen der Vorgaben der Datenschutzgesetze nicht unzulässig. Technische Unterstützung kann auch im Rahmen von Amtshilfe erfolgen, allerdings ist jegliche Verarbeitung von personenbezogenen Daten so zu organisieren, dass die Anforderungen der Datenschutzgesetze eingehalten sind.

Soweit eine (öffentliche) Stelle für eine andere die Verarbeitung der Daten auf ihren DV-Anlagen übernimmt, handelt es sich immer um eine Datenverarbeitung im Auftrag. Diese muss vertraglich geregelt werden. Da es keine bereichsspezifische Regelung gibt, ist für eine Verarbeitung von Daten des LfV insoweit § 4 HDSG maßgeblich.

§ 4 HDSG

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

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. Für ergänzende Weisungen gilt Satz 2 entsprechend. Der Auftraggeber hat zu prüfen, ob beim Auftragnehmer die nach § 10 erforderlichen Maßnahmen getroffen und die erhöhten Anforderungen bei der Verarbeitung von Daten, die besonderen Amts- oder Berufsgeheimnissen unterliegen, sowie der in § 7 Abs. 4 genannten Daten eingehalten werden. An nicht-öffentliche Stellen darf ein Auftrag nur vergeben werden, wenn weder gesetzliche Regelungen über Berufs- oder besondere Amtsgeheimnisse noch überwiegende schutzwürdige Belange entgegenstehen.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Daten-

schutzbeauftragten unterwirft. Der Auftraggeber hat den Hessischen Datenschutzbeauftragten vorab über die Beauftragung zu unterrichten.

(4) Abs. 1 bis 3 gelten auch für Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Datenverarbeitung erledigen.

Im Rahmen der Umstellung auf NADIS WN hat sich gezeigt, dass es erhebliche Schwierigkeiten bereitet, das bisherige in Hessen eingesetzte Verfahren zur Führung der Amtsdatei so weiterzuentwickeln, dass die Schnittstellt zu NADIS WN bedient werden und die notwendigen Datenübermittlungen im Rahmen des Verfassungsschutzverbundes korrekt erfolgen können. Im Ergebnis hat sich daher auch das LfV entschlossen, das Angebot des BfV anzunehmen.

Als Begründung für die Entscheidung wurde die Fehlervermeidung und im Interesse auch der Anwender die Vermeidung von Doppelerfassungen angeführt. Das LfV hat mich um Beratung gebeten, in welcher Form ich eine solche Zusammenarbeit als zulässig ansehe.

Aus meiner Sicht lassen die geltenden gesetzlichen Regelungen keine andere rechtliche Ausgestaltung als die der Auftragsdatenverarbeitung zu. Allerdings ist für meine Beurteilung der konkreten Vereinbarungen dabei nicht entscheidend, welche Bezeichnung ein solcher Vertrag hat, sondern ob die Vorgaben des § 4 HDSG zum Schutz der Rechte der Betroffenen gewahrt sind.

Dabei ist für mich in der Ausgestaltung der konkreten Vereinbarung insbesondere entscheidend, dass die Datenverarbeitung für den Auftraggeber transparent ist und dass durch diese Konstruktion die Möglichkeiten der Datenschutzkontrolle durch mich nicht verhindert werden. Dies ist durch die Gestaltung des geplanten Vertrages aus meiner Sicht sichergestellt. Die Datei wird im Aufbau NADIS WN entsprechen. Bei der Entwicklung und Pflege dieser Verbunddatei sind die Landesämter beteiligt, so dass sie auch Einfluss auf den Umfang und die Art der Datenverarbeitung nehmen können. Zudem gibt es für die Datenverarbeitung im BfV klare Regelungen insbesondere auch zu den notwendigen technischen und organisatorischen Sicherungsmaßnahmen. Deren Einhaltung wird auch durch die Bundesbeauftragte für den Datenschutz kontrolliert. Im Vertrag ist zudem festgeschrieben, dass meine Kontrollrechte von dieser Vereinbarung nicht berührt werden.

Gegenüber dem LfV habe ich im Ergebnis klargestellt, dass unabhängig von den Modifikationen, die der Vertrag mit dem BfV nunmehr enthält, es sich um eine Auftragsdatenverarbeitung handelt und nicht lediglich um Amts-

hilfe. Von einer grundsätzlich möglichen formalen Beanstandung habe ich jedoch abgesehen. Dabei ist mir bewusst, dass sich aus einem eindeutigen Vertrag zur Auftragsdatenverarbeitung ein stärkerer Einfluss des LfV auf die Tätigkeit im Rechenzentrum – von der Kontrolle bis zu einzelnen Anweisungen – ergeben würde. Ich gehe jedoch davon aus, dass unter den gegebenen Rahmenbedingungen kein zusätzliches Gefährdungspotential für die durch die Datenverarbeitung Betroffenen entsteht.

4.1.2.3
Novelle des Hessischen Sicherheitsüberprüfungsgesetzes

In diesem Jahr wurde das Hessische Sicherheitsüberprüfungsgesetz (HSÜG) novelliert. Nicht alle von mir vorgetragenen Kritikpunkte wurden berücksichtigt.

Bereits im Rahmen der Erstellung des Gesetzentwurfes hatte ich Gelegenheit, das Thema mit dem Innenministerium zu erörtern.

Dadurch konnte ich in einigen Punkten frühzeitig darauf hinwirken, dass das Recht auf informationelle Selbstbestimmung beachtet wurde. Allerdings blieben weitere Punkte offen, die ich dann auch im Rahmen einer Anhörung im Innenausschuss des Landtages vorgebracht habe.

4.1.2.3.1
Zur Frage der Notwendigkeit einer Sicherheitsüberprüfung des Hessischen Datenschutzbeauftragten

§ 3 HSÜG-E regelt, welcher Personenkreis sich einer Sicherheitsüberprüfung unterziehen muss und welcher Personenkreis darüber hinaus in die Überprüfung einbezogen wird. § 3 Abs. 4 HSÜG-E stellt demgegenüber ausdrücklich klar, für welchen Personenkreis das Gesetz keine Anwendung findet.

§ 3 Abs. 4 HSÜG-E

Dieses Gesetz gilt nicht für

1. *die Mitglieder des Hessischen Landtages, der Hessischen Landesregierung und des Staatsgerichtshofes,*
2. *Richterinnen und Richter, soweit sie Aufgaben der Rechtsprechung wahrnehmen,*
3. *ausländische Staatsangehörige, die in der Bundesrepublik Deutschland im Interesse über- oder zwischenstaatlicher Einrichtungen und Stellen eine sicherheitsempfindliche Tätigkeit nach § 1 Abs. 2 Nr. 2 ausüben sollen.*

Es entspricht der bisherigen Praxis, dass auch der jeweilige Hessische Datenschutzbeauftragte keiner Sicherheitsüberprüfung unterzogen wird.

Hintergrund dieser Praxis ist zum einen die besondere Stellung des Hessischen Datenschutzbeauftragten als unabhängige oberste Landesbehörde (§ 22 HDSG) und zum anderen die Tatsache, dass der Hessische Datenschutzbeauftragte vom Parlament gewählt und vom Präsidenten des Landtags verpflichtet wird, sein Amt gerecht und unparteiisch im Sinne der Verfassung des Landes Hessen und des Grundgesetzes der Bundesrepublik Deutschland zu führen (§ 21 HDSG). Der Hessische Datenschutzbeauftragte steht somit aufgrund seiner gesetzlichen Verpflichtungen und Aufgaben sowie seiner Entscheidungsbefugnisse, wie sie in den §§ 23 ff. HDSG auch konkretisiert werden, auf derselben Stufe wie etwa der in § 3 Abs. 4 ausgenommene Personenkreis.

Zur Klarstellung habe ich daher angeregt, dass der vom Landtag gewählte Hessische Datenschutzbeauftragte ausdrücklich in den Personenkreis aufgenommen wird, der nach § 3 Abs. 4 HSÜG-E von einer Sicherheitsprüfung ausgenommen ist.

Der Landtag ist der Auffassung gefolgt und hat auf entsprechenden Antrag hin den Hessischen Datenschutzbeauftragten in die Ausnahmeregelung mit aufgenommen.

4.1.2.3.2 Zur Möglichkeit der Anforderung einer Schufa-Auskunft beim Betroffenen

Von datenschutzrechtlicher Bedeutung war des Weiteren insbesondere die beabsichtigte Möglichkeit nach § 10 Abs. 1 S. 2 HSÜG-E, eine Datenübersicht der Schufa beim zu Überprüfenden anzufordern, wenn Hinweise auf eine finanzielle Angreifbarkeit vorliegen.

> *§ 10 Abs. 1 S. 2 HSÜG-E*
>
> *Die mitwirkende Behörde kann zusätzlich eine Datenübersicht der Schufa Holding AG nach § 34 des Bundesdatenschutzgesetzes in der Fassung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 14. August 2009 (BGBl. I S. 2814), beim zu Überprüfenden anfordern, wenn Hinweise auf eine mögliche finanzielle Angreifbarkeit des Betroffenen bestehen.*

Ich gab hier zu bedenken, dass die Regelung in dieser Form den Anforderungen an einen zulässigen Eingriff in das Recht auf informationelle Selbstbestimmung nicht gerecht wird und die Regelung daher gestrichen werden sollte. Dies bezog sich sowohl auf die Eignung und Notwendigkeit einer Schufa-Bonitätsauskunft insgesamt als auch auf die konkrete Ausgestaltung der Regelung.

Die Schufa Holding AG ist eine privatwirtschaftlich organisierte Auskunftei, die von der kreditgebenden Wirtschaft getragen wird. Ihr Geschäftszweck ist es, ihre Vertragspartner vor Kreditausfällen zu schützen. Schufa-Auskünfte erhalten grundsätzlich die Vertragspartner der Schufa, nicht jedoch dritte Stellen. Im vorliegenden Fall könnte nur die betroffene Person aufgefordert werden, eine sog. Schufa-Eigenauskunft zu beantragen und vorzulegen. Eine solche Eigenauskunft enthält eine Zusammenstellung der Informationen, die zu der betreffenden Person bei der Schufa gespeichert sind. Dies sind, neben Angaben zur Person, Daten, die von den Vertragspartnern der Schufa gemeldet worden sind, z. B. Giro- und Kundenkontoeröffnungen, Kredit- und Leasingverträge oder Telekommunikationskonten. Darüber hinaus sind ggf. von Verträgen abweichende Verhaltensweisen gespeichert, wie z. B. fällige, angemahnte und unbestrittene Forderungen. Daneben sind auch Angaben aus öffentlichen Verzeichnissen und amtlichen Bekanntmachungen aufgenommen, wie z. B. eine eidesstattliche Versicherung oder ein privates Insolvenzverfahren. Schließlich finden sich dort auch Angaben zu einem Identitätscheck im Internet.

Bereits die Tatsache, dass eine solche Auskunft gem. § 34 BDSG nur Eintragungen von Schufa-Vertragspartnern enthält und schon aus diesem Grund nie eine vollständige Übersicht über die finanziellen Verbindlichkeiten der überprüften Person bieten kann, lässt an ihrer Eignung als Grundlage der Sicherheitsüberprüfung Zweifel offen.

Darüber hinaus sind in dieser Auskunft eine Fülle von Informationen über die Betroffenen enthalten, eine Selektion dieser Eintragungen nach Relevanz im Hinblick auf eine Sicherheitsüberprüfung ist hingegen nicht möglich. So ist die Tatsache der Existenz eines Girokontos wahrscheinlich nicht sicherheitsrelevant, die Information über ein privates Insolvenzverfahren mag es sein, kann aber durch andere, öffentlich zugängliche Informationsquellen (z. B. Schuldnerverzeichnis) erworben werden.

Im Hinblick auf Sinn und Zweck der Sicherheitsüberprüfung erscheint es hingegen viel wahrscheinlicher, dass gerade mit Kreditverbindlichkeiten bei Darlehnsgebern, die nicht Mitglied der Schufa sind, ein deutlich höheres, sicherheitsrelevantes Risiko verbunden sein kann (z. B. bei Spielschulden, Wucherkrediten u. Ä.).

Die Notwendigkeit, über die Angaben aus der Sicherheitserklärung zu Krediten, Insolvenzverfahren und durchgeführten Zwangsvollstreckungen hinaus (s. § 11 Abs. 1 Nr. 11 des Gesetzentwurfs) grundsätzlich weitere Daten zu erheben, bedarf einer näheren Begründung. Abgesehen davon, dass unklar bleibt, in welchen Fällen und bei Vorliegen welcher Kriterien und Umstände „Hinweise auf eine finanzielle Angreifbarkeit des Betroffenen beste-

hen“, ist insbesondere auch nicht ersichtlich, warum nicht als Alternative eine Einsichtnahme in das Schuldnerverzeichnis als geeignetes und milderes Mittel erwogen worden ist, um eine mögliche finanzielle Angreifbarkeit der sicherheitsüberprüften Person zu prüfen.

Damit bleibt diese Regelung insgesamt zu unbestimmt und ist als Grundlage eines verfassungskonformen Eingriffs in das grundgesetzlich garantierte Recht auf informationelle Selbstbestimmung nicht geeignet. Es ist zwar einzuräumen, dass Behörden schon derzeit teilweise auf Grundlage einer Einwilligung entsprechende Auskünfte einholen, so dass der Gesetzgeber eine nachträgliche gesetzliche Legitimation dieser Praxis erwägen könnte. Die aktuelle Praxis ersetzt jedoch nicht eine Rechtfertigung des Grundrechtseingriffs. Diese fehlt gerade.

Der Landtag hat eine entsprechende Änderung des Gesetzentwurfs nicht vorgenommen.

4.1.2.3.3
Zur Notwendigkeit der Angabe einer allgemein zugänglichen eigenen Internetseite und Teilnahme in sozialen Netzwerken im Rahmen der Sicherheitserklärung

§ 11 des Entwurfs regelt, was im Einzelnen in der Sicherheitserklärung von der zu überprüfenden Person anzugeben ist. Bedenken habe ich insbesondere dagegen geäußert, dass nach § 11 Abs. 1 Nr. 17 HSÜG-E die Adresse einer allgemein zugänglichen eigenen Internetseite sowie die öffentliche Mitgliedschaft und Teilnahme in sozialen Netzwerken anzugeben ist.

§ 11 Abs. 1 Nr. 17 HSÜG-E

In der Sicherheitserklärung sind von der betroffenen Person anzugeben:

…

17. Adresse einer allgemein zugänglichen eigenen Internetseite, öffentliche Mitgliedschaft und Teilnahme in sozialen Netzwerken,

…

Ich hatte erhebliche Bedenken, dass bei einer so weiten Möglichkeit der Datenerhebung der Grundsatz der Verhältnismäßigkeit für einen zulässigen Eingriff in das Recht auf informationelle Selbstbestimmung gewahrt ist, und regte daher an, auch diese Regelung zu streichen. Mit dieser Regelung würden nämlich auch Angaben erfasst werden, die ggf. keinerlei Bezug zur Sicherheitsüberprüfung und zur konkreten Tätigkeit haben bzw. die für sich genommen keinerlei Anhaltspunkte für Sicherheitsbedenken begründen

können. Ich habe daher darauf hingewiesen, dass, sofern es sich um öffentlich zugängliche Daten handelt, welche z. B. im Rahmen einer einfachen Recherche in einer Internetsuchmaschine wie etwa bei Google erschließbar sind, die Behörde auch ohne diese Angabe des Betroffenen auf diese Informationen zugreifen könne. Im Hinblick auf Angaben zu Mitgliedschaften in sozialen Netzwerken wies ich darauf hin, dass ein zusätzlicher Informationswert überhaupt nicht gewährleistet ist, da die Betroffenen bei der Eigendarstellung in diesen Netzwerken es selbst in der Hand haben, ggf. relevante Aspekte vor einer Einsichtnahme im Rahmen der Sicherheitsüberprüfung zu verbergen.

Aber auch die Gesetzesbegründung für die Erforderlichkeit der Angaben, die im Wesentlichen auf das Zurückhaltungsgebot von Verfassungsschutzmitarbeitern verwies sowie darauf, dass durch solche Angaben das Bewusstsein des Betroffenen geschärft werden solle, war meines Erachtens nicht überzeugend. Denn selbst wenn in Bezug auf Verfassungsschutzmitarbeiter ein besonderes Bedürfnis bejaht würde, das Auftreten der Betroffenen in der Öffentlichkeit zu beobachten, so bestehen doch erhebliche Bedenken, dass dies für alle anderen zu überprüfenden Personen genauso gilt. Darüber hinaus halte ich andere Maßnahmen, wie z. B. entsprechende Hinweise und Aufklärungen z. B. im Rahmen von Einzelgesprächen, welche bei Bewerbern für den Verfassungsschutz nach der Gesetzesbegründung zu § 12 Abs. 1 HSÜG-E in jedem Fall geführt werden, zur Schärfung des Bewusstseins im Umgang mit persönlichen Daten im Internet für geeigneter.

Dem ist der Landtag jedoch ebenfalls nicht gefolgt.

4.1.3
Sozialwesen

4.1.3.1
Fehlbelegungsabgabe (Wohnungswesen) – Datenschutzrechtliche Aspekte der sozialen Wohnraumförderung

Bei der Wiedereinführung der Fehlbelegungsabgabe im Wohnungswesen durch den Landesgesetzgeber müssen bundesrechtliche Vorgaben auf dem Gebiet des Datenschutzes beachtet werden.

4.1.3.1.1
Die ministerielle Vorlage

Das Hessische Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz legte mir Ende 2014 den Entwurf eines Gesetzes über

die Erhebung der Fehlbelegungsabgabe in der sozialen Wohnraumförderung (FBAG) vor und bat mich um datenschutzrechtliche Überprüfung.

4.1.3.1.2
Datenschutzrechtliche Bewertung

In dem Gesetzentwurf (FBAG-E) war vorgesehen, dass die Kommunen die zur Durchführung des Gesetzes erforderlichen personenbezogenen Daten von bestimmten Behörden übermittelt bekommen: von Jobcentern, Sozialämtern und Versorgungsämtern (§ 4 Abs. 3 des Entwurfs). Hintergrund war, dass die entsprechenden Leistungsempfänger dieser Stellen von vornherein nicht zur Zahlung einer Fehlbelegungsabgabe verpflichtet sein sollen.

Diese Stellen, die nach dem Gesetzentwurf personenbezogene Daten übermitteln sollen, unterliegen allerdings dem speziellen im Sozialgesetzbuch geregelten Sozialdatenschutzrecht (§ 35 Abs. 2, § 68 Nr. 7 SGB I, §§ 67 ff. SGB X).

Dies hat mit Blick auf den Gesetzentwurf die rechtliche Konsequenz, dass mangels bundesgesetzlicher Übermittlungsbefugnis diese Stellen nur mit Einwilligung der Betroffenen Daten übermitteln dürfen.

§ 67b Abs. 1 S. 1 SGB X

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

An diese datenschutzrechtliche Regelung im Sozialgesetzbuch ist auch der hessische Landesgesetzgeber gebunden, weil er insoweit keine eigene Gesetzgebungskompetenz hat und folglich auch nicht zu einer Rechtsänderung befugt ist (Art. 72, 74 Abs. 1 Nr. 7 GG). In diesem Bereich der konkurrierenden Gesetzgebung hat der Bund bei der Rechtssetzung gegenüber den Ländern den Vorrang.

Davon abgesehen wurde bei der Erstellung des Gesetzentwurfs die Bedeutung der Amtshilfe rechtssystematisch offenbar überschätzt (was aus dem entsprechenden Hinweis auf die Amtshilfe in der Begründung zu § 14 Abs. 3 des Entwurfs hervorging). Das Amtshilferecht tritt, soweit es bei Sachverhaltsermittlung um personenbezogene Daten geht, hinter das Datenschutzrecht zurück (§ 3 Abs. 3 HDSG, § 1 Abs. 4 BDSG, § 37 S. 3 SGB I).

Über diese rechtlichen Vorgaben habe ich das Ministerium unterrichtet.

4.1.3.2
Kooperation von Jobcentern und anderen Stellen in der Grundsicherung für Arbeitsuchende

Die Träger der Grundsicherung für Arbeitsuchende können zu ihrer Unterstützung Dritte mit der Wahrnehmung von Aufgaben beauftragen. Sie sollen sich gegenseitig Sozialdaten übermitteln, soweit dies zur Erfüllung von Aufgaben in der Grundsicherung für Arbeitsuchende erforderlich ist. Eine Einwilligung der Betroffenen ist in diesem Fall nicht erforderlich.

4.1.3.2.1
Die ministerielle Anfrage

Das Hessische Ministerium für Soziales und Integration informierte mich Ende 2014 darüber, dass im Bereich der Grundsicherung für Arbeitsuchende („Hartz IV“) eine „Nachqualifizierungsoffensive“ für beschäftigte SGB II-Leistungsbezieher (sog. „Aufstocker“) geplant sei. Mit diesem Projekt sei auch die Zusammenarbeit von Jobcentern und Stellen verbunden, die auf dem Gebiet der Weiterbildung tätig sind (z. B. Nachqualifizierungsberatungsstellen, Weiterbildung Hessen e. V., Bildungscoachs etc.). In datenschutzrechtlicher Hinsicht sei eine individuelle Einverständniserklärung der ratsuchenden SGB II-Leistungsbezieher betreffend die Übermittlung ihrer Daten an diese Stellen vorgesehen. Vor diesem Hintergrund wurde ich um datenschutzrechtliche Überprüfung dieser vorformulierten Einverständniserklärung gebeten.

4.1.3.2.2
Datenschutzrechtliche Bewertung

In der Grundsicherung für Arbeitsuchende (SGB II) ist vorgesehen, dass sich die Träger der Grundsicherung mit Blick auf ihre Aufgabenwahrnehmung von Dritten unterstützen lassen können (§ 6 Abs. 1 S. 2 SGB II).

> *§ 6 Abs. 1 Satz 2 SGB II*
> *Zu ihrer Unterstützung können sie Dritte mit der Wahrnehmung von Aufgaben beauftragen.*

Soweit in diesem Zusammenhang die Träger der Grundsicherung Sozialdaten der Betroffenen an besagte Dritte übermitteln, kommt eine Einwilligung der Betroffenen als Rechtsgrundlage durchaus in Betracht (§ 67b Abs. 1 S. 1 SGB X).

§ 67b Abs. 1 SGB X

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

Dementsprechend ist eine Einwilligung der „Aufstocker" betreffend die Übermittlung ihrer Sozialdaten durch die Träger der Grundsicherung für Arbeitsuchende an besagte Stellen (Nachqualifizierung) entbehrlich, soweit eine gesetzliche Übermittlungsbefugnis zur Verfügung steht, und genau dies ist vorliegend der Fall, § 50 Abs. 1 SGB II.

§ 50 Abs. 1 SGB II

Die Bundesagentur, die kommunalen Träger, die zugelassenen kommunalen Träger, gemeinsame Einrichtungen ... und mit der Wahrnehmung von Aufgaben beauftragte Dritte sollen sich gegenseitig Sozialdaten übermitteln, soweit dies zur Erfüllung ihrer Aufgaben nach diesem Buch ... erforderlich ist.

Soweit die Sozialverwaltung an nicht-öffentliche Stellen Sozialdaten übermittelt, ist ein datenschutzrechtliches Problem angesprochen: Für die Sozialverwaltung gilt das sensible, bereichsspezifische Sozialdatenschutzrecht, während für nicht-öffentliche Stellen grundsätzlich das datenschutzrechtlich weniger strenge Bundesdatenschutzgesetz maßgebend ist. Der Gesetzgeber hat diesen Aspekt in der Weise kompensierend geregelt, dass nicht-öffentliche Stellen Sozialdaten nur zu dem Zweck verarbeiten und nutzen dürfen, zu dem sie von der Sozialverwaltung übermittelt worden sind (§ 78 Abs. 1 S. 1 SGB X).

§ 78 Abs. 1 Satz 1 SGB X

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

Über mein skizziertes Verständnis der Rechtslage habe ich das anfragende Ministerium informiert.

4.1.3.3
Sozialdatenschutz und Überwachung der Kommunalverwaltung durch die Stadtverordnetenversammlung

Der Sozialdatenschutz schließt die Bekanntgabe von personenbezogenen Daten an einen Ausschuss der Stadtverordnetenversammlung (Gemeinde-

vertretung) zu Zwecken der Überwachung der Kommunalverwaltung prinzipiell nicht aus.

4.1.3.3.1 Der Anlass

Das Rechtsamt einer Kommune bat mich um Auskunft, ob das Sozialamt zulässigerweise die Bekanntgabe von Sozialdaten gegenüber einem Ausschuss der Stadtverordnetenversammlung verweigern könne. Konkret ging es um den Bezug von Sozialhilfe.

4.1.3.3.2 Kommunal- und datenschutzrechtliche Bewertung

Gemäß der Hessischen Gemeindeordnung überwacht die Gemeindevertretung die gesamte Verwaltung der Gemeinde, § 50 Abs. 2 HGO.

§ 50 Abs. 2 HGO

Die Gemeindevertretung überwacht die gesamte Verwaltung der Gemeinde ... und die Geschäftsführung des Gemeindevorstandes, insbesondere die Verwendung der Gemeindeeinnahmen. Sie kann zu diesem Zweck in bestimmten Angelegenheiten vom Gemeindevorstand in dessen Amtsräumen Einsicht in die Akten durch einen von ihr gebildeten oder bestimmten Ausschuss fordern; der Ausschuss ist zu bilden oder zu bestimmen, wenn es ein Viertel der Gemeindevertreter oder eine Fraktion verlangt. Gemeindevertreter, die von der Beratung oder Entscheidung einer Angelegenheit ausgeschlossen sind (§ 25 HGO), haben kein Akteneinsichtsrecht. Die Überwachung erfolgt unbeschadet von Satz 2 durch Ausübung des Fragerechts zu den Tagesordnungspunkten in den Sitzungen der Gemeindevertretung, durch schriftliche Anfragen und aufgrund eines Beschlusses der Gemeindevertretung durch Übersendung von Ergebnisniederschriften der Sitzungen des Gemeindevorstandes an den Vorsitzenden der Gemeindevertretung und die Vorsitzenden der Fraktionen. Der Gemeindevorstand ist verpflichtet, Anfragen der Gemeindevertreter und der Fraktionen zu beantworten.

Mit Blick auf diese Kontrollbefugnisse der Gemeindevertretung gegenüber der Gemeindeverwaltung stellt sich allerdings die Frage, welche Bedeutung dem Sozialdatenschutzrecht beizumessen ist, weil die Anfrage des Rechtsamtes der Kommune eine Angelegenheit im Bereich der Sozialhilfe (SGB XII) betraf.

Ebenso wie im allgemeinen Datenschutzrecht (vgl. § 13 Abs. 4 HDSG) wird auch im Sozialdatenschutzrecht die Ausübung von Aufsichts- und Kontrollbefugnissen datenschutzrechtlich privilegiert, § 67c Abs. 3 SGB X.

§ 67c Abs. 3 SGB X

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

Allerdings betrifft diese Regelung nur die Speicherung, Veränderung oder Nutzung von Sozialdaten. Geht es – wie in der vorliegenden Angelegenheit – um die Bekanntgabe von personenbezogenen Daten durch das Sozialamt an die Gemeindevertretung, liegt datenschutzrechtlich eine Übermittlung vor und nicht nur eine behördeninterne Nutzung von personenbezogenen Daten.

Dies ergibt sich daraus, dass nicht die Kommune als solche, sondern die sozialrechtlich funktional zuständige Stelle Anknüpfungspunkt datenschutzrechtlicher Bewertungen ist, § 67 Abs. 9 S. 3 SGB X.

§ 67 Abs. 9 S. 3 SGB X

Ist der Leistungsträger eine Gebietskörperschaft, so sind eine verantwortliche Stelle die Organisationseinheiten, die eine Aufgabe nach einem der besonderen Teile dieses Gesetzbuches funktional durchführen.

Das Sozialdatenschutzrecht sieht jedoch konsequenterweise vor, dass die Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht nur bei der Speicherung, Veränderung oder Nutzung von Sozialdaten gemäß § 67c Abs. 3 SGB X privilegiert ist, sondern ebenso bei der Datenübermittlung, § 69 Abs. 5 SGB X.

§ 69 Abs. 5 SGB X

Die Übermittlung von Sozialdaten ist zulässig für die gesetzlichen Aufgaben der Rechungshöfe und der anderen Stellen, auf die § 67c Abs. 3 Satz 1 Anwendung findet.

Vor diesem Hintergrund habe ich der anfragenden Kommune mitgeteilt, dass die kommunalverfassungsrechtliche Aufgabe der Gemeindevertretung, die Gemeindeverwaltung zu überwachen, durch das Sozialdatenschutzrecht grundsätzlich nicht verhindert wird.

Allerdings habe ich auch darauf hingewiesen, dass im konkreten Einzelfall immer das Recht auf informationelle Selbstbestimmung, das Grundrechtscharakter hat (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG), und das kommunalverfassungsrechtliche Überwachungsrecht der Gemeindevertretung gegen-

einander abzuwägen sind. In diesem Zusammenhang sind insbesondere die Sensibilität der personenbezogenen Daten, die übermittelt werden sollen, und die Bedeutung der Angelegenheit für die Überwachungsfunktion der Gemeindevertretung zu berücksichtigen.

4.1.3.4
Löschung von Gesundheitsdaten beim Jobcenter

Gesundheitsdaten, die dem Jobcenter vom Gesundheitsamt unzulässigerweise übermittelt wurden, dürfen dort nicht gespeichert, sondern müssen gelöscht werden.

4.1.3.4.1
Der Anlass

Eine Bürgerin beschwerte sich bei mir darüber, dass ihre Akte beim Jobcenter (Grundsicherung für Arbeitsuchende, SGB II) Gesundheitsdaten enthalte, die vom Gesundheitsamt übermittelt worden seien. Die Daten seien aber jedenfalls teilweise für die Aufgabenwahrnehmung des Jobcenters nicht erforderlich. Zwar habe sie dem Gesundheitsamt eine Entbindung von der ärztlichen Schweigepflicht erteilt, das rechtfertige aber nicht, dass das Gesundheitsamt für das Jobcenter nicht erforderliche Gesundheitsdaten übermittele.

4.1.3.4.2
Datenschutzrechtliche Bewertung

Im Sozialrecht kann es zu den Mitwirkungspflichten des Betroffenen gehören, zu ermöglichen und einzuwilligen, dass Dritte Auskünfte geben (§ 60 Abs. 1 Nr. 1 SGB I).

> *§ 60 Abs. 1 Nr. 1 SGB I*
>
> *Wer Sozialleistungen beantragt oder erhält, hat*
> 1. *auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen ...*

Diese Obliegenheit des Betroffenen dient dazu, dem Jobcenter als Sozialleistungsträger bspw. das Recht zu geben, vom Betroffenen eine Entbindungserklärung von der ärztlichen Schweigepflicht zu verlangen. Diese ist dann die Grundlage dafür, dass das Gesundheitsamt zulässigerweise personenbezogene Daten an das Jobcenter übermitteln kann, ohne gegen

§ 203 StGB zu verstoßen, der die unbefugte Offenbarung durch Berufsgeheimnisträger unter Strafe stellt.

Typischer Fall in der Grundsicherung für Arbeitsuchende ist die ärztliche Klärung der Erwerbsfähigkeit des Betroffenen (§ 7 Abs. 1 Nr. 2 SGB II). Die Mitwirkungsobliegenheit (einzuwilligen) kann aber immer nur die für die Aufgabenwahrnehmung des Jobcenters notwendigen Informationen betreffen. Überflüssige Informationen sind also von der sozialrechtlich geforderten Einwilligung nicht gedeckt und insoweit liegt dann auch eine rechtswidrige Datenübermittlung seitens des Gesundheitsamtes an das Jobcenter vor.

Mit Blick auf den Erforderlichkeitsgrundsatz hat auch die Bundesregierung zu dem Thema „Mögliche Datenschutzprobleme im Rechtsbereich des Zweiten Buches Sozialgesetzbuch“ mit Nachdruck darauf hingewiesen, dass es keine Rechtfertigung dafür geben kann, wenn den Vermittlungskräften in den Jobcentern personenbezogene Daten der Betroffenen zur Verfügung stehen, die für die Aufgabenerfüllung irrelevant sind (BTDrucks. 17/14327, S. 6).

Ein solcher Datenschutzverstoß löst die Rechtsfolge aus, dass der Betroffene die Löschung der rechtswidrig übermittelten personenbezogenen Daten verlangen kann (§ 84 Abs. 2 Satz 1 SGB X).

§ 84 Abs. 2 Satz 1 SGB X
Sozialdaten sind zu löschen, wenn ihre Speicherung unzulässig ist.

Gemäß § 67c Abs. 1 Satz 1 SGB X ist eine Speicherung nur dann zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben nach dem Sozialgesetzbuch erforderlich ist. Genau dies trifft aber auf Informationen nicht zu, die das Jobcenter unnötigerweise vom Gesundheitsamt übermittelt bekommen hat.

Dementsprechend ordnet § 84 Abs. 2 Satz 2 SGB X konsequent die Löschung auch für solche Daten an, die zunächst für die Aufgabenerfüllung benötigt wurden, deren Erforderlichkeit dann aber entfallen ist.

Ich habe dem Landkreis diese Rechtslage mitgeteilt.

Im konkreten Fall stellte sich im Rahmen der Überprüfung allerdings heraus, dass keine Datenschutzverstöße vorlagen. Ich habe die Eingeberin darüber unterrichtet.

4.1.3.5
Datenerhebung in der Grundsicherung für Arbeitsuchende

Jobcenter sind nicht befugt, sich mit dem Hinweis, sie könnten Auskünfte jeder Art einholen, Informationen beim Vermieter des Betroffenen zu beschaffen.

4.1.3.5.1
Der Anlass

Eine Bürgerin beschwerte sich bei mir darüber, dass das für sie zuständige Jobcenter (Grundsicherung für Arbeitsuchende, SGB II) sich ohne ihre Einwilligung bei ihrem Vermieter sie betreffende Informationen besorgt habe.

Das Jobcenter, das ich deswegen um Stellungnahme bat, versuchte seine Vorgehensweise u. a. mit dem Hinweis auf § 21 SGB X (Sozialverwaltungsverfahren und Sozialdatenschutz) zu rechtfertigen. Entsprechend dieser Vorschrift sei es befugt, Auskünfte jeder Art einzuholen.

4.1.3.5.2
Datenschutzrechtliche Beurteilung

§ 21 Abs. 1 SGB X

Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere
1. Auskünfte jeder Art einholen, ...

Soweit die in § 21 SGB X angesprochene Ermittlung des Sachverhaltes personenbezogene Daten betrifft, hat diese Norm nur eine untergeordnete Bedeutung.

Dies liegt daran, dass mit Blick auf personenbezogene Daten das Sozialdatenschutzrecht vorrangig zu beachten ist und insoweit sozialverwaltungsverfahrensrechtliche Normen, wie etwa die Beweismittel betreffende Vorschrift des § 21 SGB X, verdrängt werden. Dieser Vorrang des Sozialdatenschutzes gegenüber dem Sozialverwaltungsverfahrensrecht ist gesetzlich ausdrücklich angeordnet (§ 37 SGB I).

§ 37 Satz 3 SGB I

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

Konkret heißt dies, dass insoweit das Sozialdatenschutzrecht die Regelungen des Sozialverwaltungsverfahrens verdrängt.

Dieser Vorrang des Sozialdatenschutzrechtes bedeutet allerdings nicht, dass das Jobcenter immer auf die Einwilligung des Betroffenen angewiesen ist, wenn es bei anderen Stellen personenbezogene Daten über den Betroffenen erheben will.

Aber eine solche Informationsbeschaffung muss zur Erfüllung der gesetzlichen Aufgaben des Jobcenters erforderlich sein. Anderenfalls, so hat denn auch das Bundessozialgericht entschieden, verstoßen Kontaktaufnahmen zu anderen Stellen ohne Mitwirkung des Betroffenen gegen den Datenschutz (Urteil vom 25. Januar 2012 – B 14 AS 65/11 R – RDV 2013, S. 41 ff).

Darüber hinaus ist der in § 67a SGB X festgelegte sogenannte Ersterhebungsgrundsatz zu beachten: Grundsätzlich sind Daten beim Betroffenen selbst zu erheben. Die Vorschrift enthält allerdings eine detaillierte Regelung der Ausnahmen.

Dabei kann es durchaus Konstellationen geben, in denen auch gegen den Willen des Betroffenen ein Informationsaustausch zwischen Jobcenter und Vermieter des Betroffenen erforderlich ist (z. B. § 22 Abs. 7 SGB II: direkte Zahlung seitens des Jobcenters an den Vermieter).

§ 22 Abs. 7 SGB II

Soweit das Arbeitslosengeld II für den Bedarf für Unterkunft und Heizung geleistet wird, ist es auf Antrag der leistungsberechtigten Person an den Vermieter oder andere Leistungsberechtigte zu zahlen. Es soll an den Vermieter oder andere Empfangsberechtigte gezahlt werden, wenn die zweckentsprechende Verwendung durch die leistungsberechtigte Person nicht sichergestellt ist. Dies ist insbesondere der Fall, wenn

1. *Mietrückstände bestehen, die zu einer außerordentlichen Kündigung berechtigen,*
2. *Energierückstände bestehen, die zu einer Unterbrechung der Energieversorgung berechtigen,*
3. *konkrete Anhaltspunkte für ein krankheits- oder suchtbedingtes Unvermögen der leistungsberechtigten Person bestehen, die Mittel zweckentsprechend zu verwenden, oder*
4. *konkrete Anhaltspunkte dafür bestehen, dass die im Schuldnerverzeichnis eingetragene leistungsberechtigte Person die Mittel nicht zweckentsprechend verwendet.*

Der kommunale Träger hat die leistungsberechtigte Person über eine Zahlung der Leistungen für die Unterkunft und Heizung an den Vermieter oder andere Empfangsberechtigte schriftlich zu unterrichten.

Mit dem Thema Vorlage des Mietvertrages bzw. einer Vermieterbestätigung durch den Betroffenen beim Jobcenter habe ich mich bereits im 42. Tätigkeitsbericht (Ziff. 3.3.7.3) ausführlich befasst.

Das Jobcenter habe ich über die Rechtslage unterrichtet.

Im konkreten Fall war es so, dass auch nach Maßgabe des Sozialdatenschutzes die Eingeberin nicht in ihren Rechten verletzt wurde. Das habe ich gegenüber der Eingeberin näher ausgeführt.

4.1.3.6
Verantwortlichkeit für Datenübermittlungen an die Sozialverwaltung

Grundsätzlich trägt die Stelle, die Daten übermittelt, die Verantwortung für die Rechtmäßigkeit der Datenübermittlung. Beruht die Datenübermittlung auf dem Ersuchen eines Dritten, ist dieser verantwortlich für die Richtigkeit seiner Angaben und insoweit auch für die Zulässigkeit der Datenübermittlung.

4.1.3.6.1
Die Anfrage

Die Geschäftsführung einer Klinik bat mich um Auskunft zu folgender Thematik:

An die Klinik würden regelmäßig Auskunftsbegehren von Behörden gerichtet, die – zwecks Beurteilung im Rahmen von Feststellungsverfahren nach dem Schwerbehindertenrecht – die Herausgabe von Patientenakten bzw. Entlassungsberichten beträfen.

Die Behörden, so die Klinik, würden lediglich versichern, dass eine schriftliche Einverständniserklärung der betroffenen Patienten vorliege, nicht aber eine Kopie einer solchen Erklärung der Patienten ihrem Auskunftsbegehren beifügen.

Für die Klinik stelle sich die Frage, ob sie auf die Vorlage der schriftlichen Einverständniserklärung der Patienten in Kopie oder im Original bestehen müsse.

4.1.3.6.2
Datenschutzrechtliche Bewertung

Im Sozialrecht ist die Übermittlungsverantwortung in § 67d Abs. 2 SGB X recht knapp geregelt.

§ 67d Abs. 2 SGB X

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

Diese Vorschrift betrifft allerdings die Konstellation, dass sozialrechtliche Leistungsträger (§ 35 SGB I) Daten übermitteln, und nicht wie vorliegend, dass SGB-Stellen Empfänger der Datenübermittlungen durch Kliniken sind.

Maßgebend für die Datenübermittlung von Krankenhäusern ist vielmehr § 12 Abs. 1 Hessisches Krankenhausgesetz, der auf den hier interessierenden § 14 HDSG verweist.

Diese Vorschrift regelt die Frage der Übermittlungsverantwortung etwas differenzierter als der oben genannte § 67d Abs. 2 SGB X (ausführlich zu § 14 HDSG Dembowski in Schild/Ronellenfitsch u. a.).

§ 14 HDSG

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben eines Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

Ich habe die Geschäftsführung der anfragenden Klinik dementsprechend informiert. Vor diesem gesetzlichen Hintergrund kann sie sich grundsätzlich darauf verlassen, dass die Sozialverwaltung die von der Klinik angeforderten Unterlagen für ihre gesetzliche Aufgabenwahrnehmung nach Maßgabe des Sozialgesetzbuchs benötigt und dass die erforderlichen Entbindungserklärungen der Betroffenen von der ärztlichen Schweigepflicht vorliegen.

4.1.4
Gesundheit

4.1.4.1
Ausgestaltung von Schweigepflichtentbindungserklärungen der Gutachter- und Schlichtungsstelle bei der Landesärztekammer Hessen

Das pauschale Musterformular der Landesärztekammer Hessen zur Entbindung von der Schweigepflicht im Rahmen von Gutachter- und Schlichtungsverfahren wurde meinen Anforderungen entsprechend datenschutzgerecht gestaltet.

4.1.4.1.1
Die alte Fassung

Auf das Formular der Landesärztekammer Hessen hat mich ein Petent aufmerksam gemacht, der die Behandlung durch einen hessischen Augenarzt von der Landesärztekammer überprüfen lassen wollte.

Bemängelt wurde von ihm insbesondere, dass in dem Formular pauschal alle beteiligten Personen (d. h. „Ärzte und sonstige Personen“) von der Schweigepflicht entbunden wurden. Eine Einschränkung auf einen konkreten Fall (Behandlungszeitraum, Behandlungsmaßnahme etc.) war dem Dokument dahingegen nicht zu entnehmen.

Ebenso wurde beanstandet, dass die vom Eingebenden selbst verfasste Schweigepflichtentbindungserklärung nicht von der Kammer akzeptiert wurde. Dies hatte im Übrigen dazu geführt, dass der Betroffene seinen Antrag gegenüber der Schlichtungsstelle zurückgezogen hat.

Das alte Formular sah auch vor, dass ein Widerruf der Einwilligungserklärung generell zum Abbruch des Verfahrens führt.

4.1.4.1.2
Die neue Fassung

Ich habe die Kammer davon überzeugen können, dass das Formular mit Freitextfeldern zu versehen ist, damit der Anlass der Schweigepflichtentbindung noch einmal konkretisiert werden kann. So ist insbesondere die „beanstandete Behandlung“ näher anzuführen (Benennung der Operation/Diagnose, Zeitpunkt/Zeitraum der Behandlung, behandelnder Arzt/Ärztin etc.). Vor allem die Stellen, von denen die Informationen angefordert werden, müssen im Vorfeld möglichst genau wissen, welche Daten sie aufgrund der Entbindung von der Schweigepflicht herausgeben dürfen.

Nach meinen Vorgaben ist auch die Möglichkeit vorzusehen, dass der Betroffene eine selbst verfasste/ergänzte Schweigepflichtentbindungserklärung einreichen kann, in welcher auch die Namen derjenigen Ärzte oder Einrichtungen einzeln aufgeführt werden können, die von der Schweigepflicht entbunden werden sollen. Für gelungen halte ich insoweit das Muster der Gutachterstelle für Arzthaftungsfragen bei der Bayerischen Landesärztekammer, dem zusätzlich ein erläuterndes Merkblatt beigefügt wird.

Dem dadurch gegebenenfalls entstehenden, erhöhten Verwaltungsaufwand kann dadurch Rechnung getragen werden, dass auf eine mögliche Verzögerung des Verfahrens hingewiesen wird.

Aufgrund dieser vorgenommenen Änderungen habe ich auch erreichen können, dass der Widerruf der Einwilligungserklärung in Anbetracht der nunmehr möglichen Einzel-Schweigepflichtentbindungen nicht in allen Fällen zum Abbruch des Verfahrens führen **muss.** Es wird jetzt darauf hingewiesen, dass Entsprechendes zu einem Abbruch des Verfahrens führen **kann.** Hierdurch lässt sich auch vermeiden, dass von dem Widerrufsrecht nur deshalb nicht Gebrauch gemacht wird, weil eine Verfahrenseinstellung die zwingende Folge wäre.

4.1.5
Kommunale Selbstverwaltung

4.1.5.1
Ausstattung von Bürgerbüros

Bürgerbüros müssen so eingerichtet werden, dass Bürgerinnen und Bürger die Möglichkeit haben, ihre Anliegen einem Mitarbeiter der Verwaltung so vorzutragen, dass Dritte nicht mithören können.

Immer wieder erreichen meine Dienststelle Beschwerden von Bürgerinnen und Bürgern über die Einrichtung von Bürgerbüros. Regelmäßig wird eingewandt, dass es in den Bürgerbüros nicht möglich sei, den Mitarbeiterinnen und Mitarbeitern der Verwaltung persönliche Daten mitzuteilen, ohne dass andere Besucher des Bürgerbüros mithören können. Oft stelle ich bei meinen Überprüfungen fest, dass diese Beschwerden durchaus berechtigt sind. Exemplarisch seien hier zwei große Bürgerbüros Hessens genannt, in denen ein vertrauliches Gespräch mit Mitarbeitern der Verwaltung nahezu unmöglich war. Dies betraf zum einen das Bürgerbüro im Luisenforum in Wiesbaden und zum anderen das Bürgerbüro im Rathaus in Kassel.

In Wiesbaden waren die Stühle des Wartebereichs für Antragsteller/Auskunftssuchende so angeordnet, dass sie direkt hinter den Besuchern, die bereits am Schalter bedient wurden, platziert waren. Damit ließ sich gar nicht vermeiden, dass sie die Gespräche an den Schaltern verfolgen konnten. Eine Person, die wartet und sonst nichts zu tun hat, wird zwangsläufig einem Gespräch folgen, das unmittelbar vor oder neben ihr geführt wird. Hier habe ich in persönlichen Gesprächen mit Verantwortlichen des Bürgerbüros erreichen können, dass die Anordnung des Wartebereichs verändert wurde, so dass die Mithörsituation aufgehoben wurde. Inzwischen ist die räumliche Situation datenschutzfreundlich gelöst.

In Kassel standen die einzelnen Arbeitsplätze sehr nah beieinander und zum Zeitpunkt meines Besuchs waren auch beinahe alle besetzt. Da mehrere

Außenstellen von Bürgerbüros wegfallen sollten, war davon auszugehen, dass auch in Zukunft immer alle Plätze besetzt sein werden. Unter diesen Bedingungen ließ sich gar nicht vermeiden, dass die Bürger die Anliegen anderer Bürger an den Nebenarbeitsplätzen mitbekommen. Hier habe ich als ersten Schritt für die Verbesserung der Situation vorgeschlagen, dass das Angebot unterbreitet wird, dass Gespräche auch in einem separaten Raum geführt werden können. Dieser Vorschlag wurde befolgt. Inzwischen ist das Bürgerbüro umfangreich umgebaut worden. Bei dem Umbau wurden in besonderem Maße auch die Belange der Bürgerinnen und Bürger an einem ungestörten Dialog mit der Verwaltung berücksichtigt. Die Arbeitsplätze wurden entzerrt und es besteht weiterhin das Angebot, Anliegen unter vier Augen in einem getrennten Raum zu besprechen. Dieses Angebot wird für jeden Besucher gut sichtbar als Fußzeile an den Monitoren angezeigt, auf denen der Hinweis, welche gezogene Nummer zu welchem Arbeitsplatz zugeordnet ist, angezeigt wird.

„Willkommen im Bürgerbüro Kassel. Wünschen Sie mehr Diskretion? Es besteht die Möglichkeit, dass Sie in einem abgetrennten Bereich des Bürgerbüros bedient werden. Sprechen Sie uns an. Ab sofort können Sie Termine im Bürgerbüro Mitte vereinbaren. Nutzen Sie die Möglichkeit online auf der Internetseite der Stadt Kassel, telefonisch unter der Behördennummer 115 oder direkt im Bürgerbüro am Infoschalter.“

Die Umbaumaßnahme hat in herausragender Weise zu einer Verbesserung der datenschutzrechtlichen Situation geführt.

Da auch bei der Stadt Wiesbaden Informationsmonitore installiert sind, habe ich angeregt, dass diese Art der Information auch dort übernommen wird. Diese Anregung wurde daraufhin übernommen.

4.1.5.2
Übermittlung von Meldedaten an die Bundeswehr

Gegen die Übermittlung von Meldedaten an das Bundesamt für das Personalmanagement der Bundeswehr steht den Betroffenen ein Widerspruchsrecht zu.

Die Eltern eines 17-jährigen Mannes haben sich an meine Dienststelle gewandt und sich darüber beschwert, dass ihr Sohn von der Bundeswehr angeschrieben und auf die Berufsmöglichkeiten bei der Bundeswehr aufmerksam gemacht wurde. Die Bundeswehr habe in ihrem Schreiben darauf hingewiesen, dass sie zu „Werbezwecken" Daten Nichtvolljähriger von den Einwohnermeldeämtern übermittelt bekommen dürfe. Die Eltern des 17-Jährigen waren der Auffassung, dass eine Weitergabe der Daten ihres minderjährigen Sohnes ohne ihre Einwilligung als Erziehungsberechtigte datenschutzrechtlich nicht zulässig ist.

Bis zum Jahr 2011 erfolgte eine Datenübermittlung der Einwohnermeldeämter an die Bundeswehr aufgrund von § 15 Wehrpflichtgesetz. Dort ist geregelt, dass die Wehrerfassungsbehörde die Daten des Melderegisters nutzen darf, soweit dies zur Feststellung der Wehrpflicht erforderlich ist. Mit dem Wehrrechtsänderungsgesetz des Jahres 2011 wurde die Geltung auch dieser Norm ausgesetzt und gem. § 2 auf den Spannungs- oder Verteidigungsfall begrenzt, so dass eine Datenübermittlung nicht mehr auf diese Norm gestützt werden kann.

Allerdings hat der Gesetzgeber mit § 58c Soldatengesetz der Bundeswehr die Möglichkeit eingeräumt, gezielt über die Tätigkeit in den Streitkräften zu informieren. Zu diesem Zweck übermitteln die Meldebehörden jährlich bis zum 31. März Familienname, Vorname und gegenwärtige Anschrift der Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden.

§ 58c SG

(1) Zum Zweck der Übersendung von Informationsmaterial nach Absatz 2 Satz 1 übermitteln die Meldebehörden dem Bundesamt für das Personalmanagement der Bundeswehr jährlich bis zum 31. März folgende Daten zu Personen mit deutscher Staatsangehörigkeit, die im nächsten Jahr volljährig werden:

1. Familienname,
2. Vorname,
3. gegenwärtige Anschrift.

Die Datenübermittlung unterbleibt, wenn die Betroffenen ihr nach § 18 Absatz 7 des Melderechtsrahmengesetzes widersprochen haben.

(2) Das Bundesamt für das Personalmanagement der Bundeswehr darf die Daten nur dazu verwenden, Informationsmaterial über Tätigkeiten in den Streitkräften zu versenden.

(3) Das Bundesamt für das Personalmanagement der Bundeswehr hat die Daten zu löschen, wenn die Betroffenen dies verlangen, spätestens jedoch nach Ablauf eines Jahres nach der erstmaligen Speicherung der Daten beim Bundesamt für das Personalmanagement der Bundeswehr.

Um den Interessen der Betroffenen gleichwohl Rechnung zu tragen, wurde ein Widerspruchsrecht gegen diese Datenübermittlungen in das Gesetz aufgenommen. Wenn der Meldebehörde kein Widerspruch gegen die Datenübermittlung an das Bundesamt vorliegt, ist sie berechtigt, diese Daten zu den oben aufgeführten Zwecken an die Bundeswehr weiterzugeben.

Junge Frauen und Männer, die kein Informationsmaterial von der Bundeswehr erhalten möchten, sollten deshalb frühzeitig (im Alter von 16 Jahren) dieser Datenübermittlung bei ihrer zuständigen Einwohnermeldebehörde widersprechen.

Als weiteres Betroffenenrecht hat der Gesetzgeber auch einen jederzeitigen Löschungsanspruch der Betroffenen ins Gesetz aufgenommen. Ich habe daher den Eltern empfohlen, dass ihr Sohn von seinem Löschungsanspruch nach § 58c Soldatengesetz unverzüglich Gebrauch macht.

4.1.5.3
Keine Speicherung von Dissertationsurkunden und Scheidungsurteilen in Meldebehörden

Beantragte Veränderungen im Einwohnermelderegister müssen nur im erforderlichen Umfang belegt werden. In der Regel reicht dabei für die Meldebehörde der Vermerk aus, dass das entsprechende Dokument vorgelegen hat.

Immer wieder erreichen mich Anfragen von Bürgern, die befürchten, dass Einwohnermeldeämter mehr Informationen anfordern oder speichern, als dies zur Aufgabenerfüllung eines Meldeamtes erforderlich ist.

So wurde eine Bürgerin aufgefordert, zum Nachweis ihres geänderten Familienstandes dem Einwohnermeldeamt ein komplettes Scheidungsurteil vorzulegen. Da ein Scheidungsurteil viele persönliche Informationen ent-

hält, die für die Arbeit eines Meldeamtes keine Relevanz haben, konnte die Bürgerin dafür kein Verständnis aufbringen.

In einem anderen Fall beschwerte sich eine Bürgerin, dass ein Einwohnermeldeamt eine Kopie ihrer Dissertationsurkunde für die Meldeunterlagen fertigte, nachdem sie die Führung ihres neu erworbenen Doktortitels in ihrem Personalausweis beantragt hatte. Eine Dissertationsurkunde enthält neben dem Tag des Erwerbs des Doktortitels und der Universität auch Informationen zum Thema, der Benotung sowie den Namen des betreuenden Professors der Doktorarbeit.

Der Datenumfang der Einwohnermelderegister ist in § 3 HMG abschließend festgelegt. Über die als „Daten“ bezeichneten Angaben hinaus dürfen die Meldebehörden auch die zum Nachweis der Richtigkeit erforderlichen Hinweise speichern. Hierbei handelt es sich um die Benennung von Urkunden und Nachweisen mit Bezeichnung der ausstellenden Behörde oder des Gerichts mit Aktenzeichen und Tag der Ausstellung sowie Tag des Ereignisses. Die Erforderlichkeit nach § 11 HDSG ist trotzdem zu beachten, um den Einzelnen gegen die unbegrenzte Erhebung und Speicherung von persönlichen Daten zu schützen.

Die Einwohnermeldedatei ist die Basis für viele behördliche Entscheidungen. Die Richtigkeit aller dort gespeicherten Angaben ist daher Voraussetzung für ein geordnetes Verwaltungshandeln. Trotzdem darf die heute einfache Verfügbarkeit von Kopierern nicht dazu führen, dass mehr personenbezogene Daten im Einwohnermeldeamt gespeichert werden, als dies zur Aufgabenerfüllung erforderlich ist. Regelmäßig genügt zum Nachweis der Richtigkeit ein Vermerk darüber, dass die entsprechende Urkunde oder das Gerichtsurteil vorgelegen hat, ergänzt um die oben ausgeführten Daten.

Für den Nachweis einer rechtskräftigen Scheidung gegenüber Behörden genügt der Tenor der Gerichtsentscheidung. Zur Vorlage von Scheidungsurteilen bei einer erneuten Eheschließung habe ich dies in meinem 37. Tätigkeitsbericht (Ziff. 5.5) bereits ausführlich ausgeführt. Ebenso halte ich die Aufbewahrung einer Kopie der Dissertationsurkunde im Einwohnermeldeamt für nicht erforderlich. Die anfragenden Bürger und die jeweils zuständigen Einwohnermeldeämter wurden über meine Rechtsauffassung informiert.

4.1.5.4
Fragebogen zur Anmeldung einer Nebenwohnung

Einige Kommunen nutzen bei der Anmeldung von Nebenwohnungen zusätzliche Fragebögen. Der Umfang eines solchen Fragebogens muss auf das erforderliche Maß beschränkt werden.

Die Beschwerde eines Bürgers über detaillierte Fragen in einem Fragebogen zur Anmeldung einer Nebenwohnung veranlasste mich, das Verfahren erneut zu prüfen.

Das Hessische Meldegesetz bestimmt in § 16, dass für einen Einwohner oder eine Einwohnerin mit mehreren Wohnungen im Inland die vorwiegend genutzte Wohnung der Hauptwohnsitz ist.

§ 16 HMG

(1) Hat eine Einwohnerin oder ein Einwohner mehrere Wohnungen im Inland, so ist eine dieser Wohnungen die Hauptwohnung.

(2) Hauptwohnung ist die vorwiegend benutzte Wohnung der Einwohnerin oder des Einwohners. Hauptwohnung einer verheirateten Einwohnerin oder eines verheirateten Einwohners oder einer eine eingetragene Lebenspartnerschaft führenden Einwohnerin oder eines eine eingetragene Lebenspartnerschaft führenden Einwohners, die oder der nicht dauernd getrennt von ihrer oder seiner Familie oder ihrer Lebenspartnerin oder seines Lebenspartners lebt, ist die vorwiegend benutzte Wohnung der Familie oder der Lebenspartnerin oder des Lebenspartners. Hauptwohnung einer minderjährigen Einwohnerin oder eines minderjährigen Einwohners ist die vorwiegend benutzte Wohnung der oder des Personensorgeberechtigten. Leben diese getrennt, ist Hauptwohnung die Wohnung der oder des Personensorgeberechtigten, die von der oder dem Minderjährigen vorwiegend benutzt wird. Hauptwohnung eines behinderten Menschen, der in einer Behinderteneinrichtung untergebracht ist, bleibt auf Antrag des behinderten Menschen bis zur Vollendung des 27. Lebensjahres die Wohnung nach Satz 3. In Zweifelsfällen ist die vorwiegend benutzte Wohnung dort, wo der Schwerpunkt der Lebensbeziehungen der Einwohnerin oder des Einwohners liegt. Kann der Wohnungsstatus einer verheirateten Einwohnerin oder eines verheirateten Einwohners oder einer eine eingetragene Lebenspartnerschaft führenden Einwohnerin oder eines eine eingetragene Lebenspartnerschaft führenden Einwohners nach Satz 2 und 6 nicht zweifelsfrei bestimmt werden, ist die Hauptwohnung die Wohnung nach Satz 1.

(3) Nebenwohnung ist jede weitere Wohnung.

(4) Die Einwohnerin oder der Einwohner hat bei jeder An- oder Abmeldung mitzuteilen, welche weiteren Wohnungen sie oder er hat und welche Wohnung die Hauptwohnung ist. Der Meldebehörde der neuen Hauptwohnung ist jede Änderung der Hauptwohnung mitzuteilen. Die Änderung kann auch der für eine Nebenwohnung zuständigen Meldebehörde zur Weiterleitung an die zuständige Meldebehörde mitgeteilt werden.

Bei verheirateten oder in einer eingetragenen Lebenspartnerschaft lebenden Einwohnern ist die vorwiegend benutzte Wohnung der Familie der Hauptwohnsitz. Eine Wahlmöglichkeit der Einwohnerin oder des Einwohners mit mehreren Wohnungen besteht nicht. Wesentlich für die Anerkennung einer Wohnung als Hauptwohnung ist die zeitliche Nutzungsdauer. Wobei hier der tatsächliche Aufenthalt an dem Wohnort und nicht die Nutzungsdauer der Wohnung maßgeblich ist.

Gerade Studentinnen und Studenten erklären häufig den Wohnsitz ihrer Eltern zum Hauptwohnsitz, weil sie ihren Aufenthalt am Standort ihrer Universität nur als vorübergehend betrachten. Für Universitätsstädte bedeutet dies, dass viele Einwohner ihre Infrastruktur nutzen, die dann bei der Zuweisung von Finanzmitteln aber keine Rolle spielen. Erfahrungsgemäß überprüfen daher diese Städte sehr viel gründlicher die Voraussetzungen für die Anmeldung einer Nebenwohnung.

Meine Umfrage bei verschiedenen Kommunen mit einer Universität oder Hochschule ergab, dass dieses Problem unterschiedlich gelöst wurde. Eine Stadt hatte nach Einführung einer Zweitwohnungssteuer keine Probleme mehr mit angemeldeten Nebenwohnungen. Eine andere Stadt nimmt Studenten grundsätzlich mit Hauptwohnung in das Einwohnermelderegister auf. Wird trotzdem die Anmeldung mit einer Nebenwohnung gewünscht, müssen die Gründe und Aufenthaltszeiten hierfür gegenüber der Meldestelle eindeutig dargelegt werden. In drei Kommunen sind bei der Anmeldung einer Nebenwohnung Fragebogen auszufüllen. Zwei Fragebogen enthielten hierbei Fragen zum genutzten Verkehrsmittel für Heimfahrten, zu ausgeübten Tätigkeiten oder zur Ausbildungsart, die nach meiner Ansicht für die Bestimmung eines Hauptwohnsitzes nicht erforderlich und daher nach § 11 HDSG unzulässig sind.

Mittlerweile wurde das Problem in einer Arbeitsgruppe der hessischen Großstädte gemeinsam mit dem Innenministerium erörtert und die Handhabung abgestimmt. Sollte sich nach den Angaben der Betroffenen bei der persönlichen Anmeldung keine Hauptwohnung bestimmen lassen, werden in einem schriftlichen Verfahren die melderechtlichen Fragen ohne Fragebogen geklärt.

4.1.5.5
Gebührenfreie Auskunft durch Standesämter

Auch Standesämter sind verpflichtet, Bürgern schriftlich gebührenfreie Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen.

Ein Bürger hatte sich an ein hessisches Standesamt gewandt und begehrte schriftliche Auskunft über die Daten, die im Geburtsregister über ihn eingetragen waren. Das Standesamt hat die Auffassung vertreten, dass eine Auskunft über die zu einer Person im Standesamt gespeicherten Daten nur im Wege der Urkundserteilung möglich sei. Diese sei zwangsläufig gebührenpflichtig. Die Nutzung der Personenstandsbücher sei in § 62 Personenstandsgesetz (PStG) abschließend geregelt. Danach seien für eine schriftliche Auskunftserteilung grundsätzlich Gebühren vorgesehen. Die Benut-

zungsbestimmungen des Personenstandsgesetzes gingen insofern den Datenschutzgesetzen der Länder, die das Recht auf gebührenfreie Auskunft enthielten, vor.

§ 18 Abs. 3 HDSG

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

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

Die Datenschutzbeauftragte der Kommune wandte sich daraufhin an meine Dienststelle und bat um meine rechtliche Einschätzung, ob das Auskunftsrecht des § 18 Abs. 3 HDSG auch das Recht umfasse, einen gebührenfreien Ausdruck von einem Standesamt zu erhalten.

Ich habe diese Frage bejaht. Das Auskunftsrecht nach § 18 Abs. 3 HDSG wie auch das Akteneinsichtsrecht nach § 18 Abs. 5 HDSG dient dazu, den Betroffenen in die Lage zu versetzen, sich gegebenenfalls rechtlich mit der Datenspeicherung auseinandersetzen zu können. Dies geht nur, wenn der Betroffene auch etwas Schriftliches in der Hand hat (siehe insoweit auch Ziff. 3.1.2 in meinem 40. Tätigkeitsbericht).

Wenn das Fachverfahren, das in der Kommune zum Einsatz kommt, nur den Ausdruck in Form von gebührenpflichtigen Urkunden zulässt, dann ist die schriftliche Auskunft in anderer Form zu erteilen. Dieses Problem besteht durchaus auch in anderen Fachverfahren. Auch hier werden dann die Auskünfte in einem eigens zu erstellenden Brief erteilt.

Der Anspruch auf Auskunft über die bei einer öffentlichen Stelle vorhandenen personenbezogenen Daten ist Ausfluss des Grundrechts auf informationelle Selbstbestimmung. Dieser Anspruch darf grundsätzlich nicht durch Gebühren unmöglich gemacht oder erschwert werden. Bei § 62 Abs. 1 und 2 PStG handelt es sich um eine spezialgesetzliche Auskunftsregelung, die eng zu verstehen ist. Die Legitimation des Standesamtes, für eine Auskunft nach PStG eine Gebühr zu erheben, ergibt sich danach nur für die Erstellung einer Urkunde. Für die sonstige Auskunftserteilung bleibt es bei der Gebührenfreiheit. Das Hessische Datenschutzgesetz mit § 18 Abs. 3 geht hier als die Verfassung konkretisierende Vorschrift vor.

4.1.5.6
Auskünfte an Immobilienmakler über Grundstückseigentümer

Immobilienmakler müssen bei ihren Ersuchen an die Ämter für Bodenmanagement nach Auskunft von Daten über Grundstückseigentümer das Vorliegen eines berechtigten Interesses im Sinne des Vermessungs- und Geoinformationsgesetzes substanziiert darlegen.

Die bei den Ämtern für Bodenmanagement geführten Liegenschaftskataster sind öffentliche Register, die jeder Person zur Einsicht und Auskunft offenstehen. Die Auskunft kann über Einzelanfragen gewährt werden. Es besteht auch die Möglichkeit der Teilnahme an einem automatisierten Abrufverfahren. In meinem letzten Tätigkeitsbericht (42. Tätigkeitsbericht, Ziff. 3.3.10.1) wurde auf die Problematik der Erteilung von Auskunft über die Eigentümerdaten an Personen der Immobilienvermittlung durch die Ämter für Bodenmanagement eingegangen. Dabei wurde das Augenmerk auf die Ausgestaltung von automatisierten Abrufverfahren und deren Kontrolle durch die Liegenschaftsverwaltung gelegt. In diesem Beitrag wird der Fokus auf die Einzelanfragen der Personen der Immobilienvermittlung nach Eigentümerdaten direkt bei den Ämtern für Bodenmanagement gerichtet.

Die Einsicht in die Namen, die Geburtsdaten und die Anschriften der Eigentümer steht nach § 16 Abs. 2 des Hessischen Gesetzes über das öffentliche Vermessungs- und Geoinformationswesen (HVGG) nur den Personen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben.

§ 16 Abs. 1 bis 3 HVGG

(1) Jede Person oder Stelle kann die Datenbanken des öffentlichen Vermessungswesens als allgemein zugängliche Quellen einsehen sowie Auskünfte oder Ausgaben daraus erhalten.

(2) Abweichend von Abs. 1 stehen die Einsicht in die Namen, die Geburtsdaten und die Anschriften der Eigentümerinnen und Eigentümer sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Entsprechendes gilt für die Daten der Bevollmächtigten. Das berechtigte Interesse ist darzulegen. Die Empfänger dürfen diese Daten nur für den Zweck nutzen, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden. Satz 3 gilt nicht für

1. *dinglich Berechtigte,*
2. *Behörden des Landes und kommunale Gebietskörperschaften in Erfüllung ihrer Aufgaben,*
3. *Öffentlich bestellte Vermessungsingenieurinnen und Vermessungsingenieure sowie Notarinnen und Notare, soweit die personenbezogenen Daten im Einzelfall zur Erfüllung ihrer Aufgaben benötigt werden.*

(3) Die digitalen Datenbanken des öffentlichen Vermessungswesens sollen mittels geeigneter, öffentlich verfügbarer Telekommunikationsmittel nutzbar sein.

Als „berechtigtes Interesse“ wird grundsätzlich jedes sachbezogene persönliche, wissenschaftliche, statistische, historische, rechtliche und auch wirtschaftliche Interesse, das über ein allgemeines, unspezifiziertes Informationsinteresse oder die reine Neugier hinausgeht, anerkannt. In diesem Zusammenhang stellt sich die Frage, in welchen Konstellationen von dem Vorliegen eines solchen berechtigten Interesses bei Personen der Immobilienvermittlung auszugehen ist und welche Anforderungen an die Darlegungspflicht zu stellen sind.

Immobilienmakler haben für sich allein kein berechtigtes Interesse an der Kenntnis der Namen, Geburtsdaten und Anschriften der im Liegenschaftskataster geführten Eigentümer. Der bloße Hinweis auf ihre berufliche Tätigkeit begründet noch kein berechtigtes Interesse im Sinne von § 16 Abs. 2 HVGG.

Ein wirtschaftliches Interesse an der Kenntnis der Eigentümerdaten ist aber anzuerkennen, wenn der Makler von einem bestimmten Interessenten beauftragt worden ist, Kontakt wegen des Verkaufs eines oder mehrerer Grundstücke herzustellen. Mit dieser Rechtsauffassung bin ich an das Landesamt für Bodenmanagement und Geoinformation herangetreten und bat um Überprüfung der Auskunftspraxis gegenüber Personen der Immobilienvermittlung. Wir einigten uns darauf, dass die Makler nach substanziierter Darlegung eines konkreten Vermittlungsauftrages eine Auskunft über die Eigentümerdaten erhalten dürfen. Eine substanziierte Darlegung liegt beispielsweise dann vor, wenn die Antrag stellende Person ihr internes Geschäftszeichen des Vermittlungsauftrages angibt.

Dabei muss der Auskunft erteilende Bedienstete des Amtes für Bodenmanagement nach sorgfältiger Prüfung der vorgetragenen Umstände das Datum, seinen Namen, den Namen des Antragstellers, die Ortungskriterien der betroffenen Grundstücke (z. B. Gemarkung, Flur, Flurstück) sowie alle wesentlichen Angaben zum dargelegten berechtigten Interesse aktenkundig machen und zwei Jahre aufbewahren. Mir muss nach § 29 Abs. 1 HDSG zur Prüfung der rechtmäßigen Auskunftserteilung Auskunft aus diesen Aufzeichnungen gegeben werden. Ich behalte mir das Recht vor, die von den Maklern gegenüber den Ämtern für Bodenmanagement gemachten Angaben zu überprüfen.

4.1.5.7
Überprüfung schon länger bestehender Anlagen zur Videoüberwachung

Betreiber von Videoüberwachungsanlagen müssen die Zulässigkeit alle zwei Jahre überprüfen. Eine wesentliche Reduktion der Anzahl der betriebenen Videoüberwachungsanlagen durch diese Überprüfungen habe ich allerdings nicht festgestellt.

Zum Zeitpunkt der Installation von Videoüberwachungsanlagen durch Gefahrenabwehrbehörden müssen die Voraussetzungen des § 14 Abs. 4 HSOG erfüllt sein. Dies bedeutet, dass Videoüberwachungsanlagen auf öffentlichen Straßen und Plätzen nur zulässig sind, wenn dort wiederholt Straftaten begangen worden sind und tatsächliche Anhaltspunkte für weitere Straftaten bestehen oder die Videoüberwachungsanlage zum Schutz besonders gefährdeter öffentlicher Einrichtungen dient. Fest installierte Videokameras dürfen dann zwei Jahre ohne weitere Prüfung betrieben werden. Alle zwei Jahre ist eine erneute Prüfung der Voraussetzungen in § 14 Abs. 4 Satz 3 HSOG vorgeschrieben.

Mitte des Jahres habe ich 14 Kommunen angeschrieben, die bereits seit 2012 oder früher Videoüberwachungsanlagen betreiben, und um Mitteilung des Ergebnisses einer solchen Überprüfung gebeten.

In der Regel begründen die Kommunen die Videoüberwachung damit, dass Straftaten, insbesondere Sachbeschädigungen von öffentlichem Eigentum verhindert werden sollen. Da sich die räumlichen Gegebenheiten in Kommunen nach einem Zeitraum von zwei Jahren selten verändern, sahen alle befragten Kommunen den weiteren Betrieb der Videoüberwachungsanlagen für weitere zwei Jahre als zwingend notwendig an. Den durch die Videoüberwachung erreichten oder vermuteten Rückgang der Kriminalität bzw. Sachbeschädigungen wolle man durch einen Abbau der Videokameras nicht gefährden.

Nur drei Kommunen hatten zur Prüfung der weiteren Rechtmäßigkeit des Betreibens der Videoanlagen auch Stellungnahmen der Polizei bzw. des Ordnungsamtes eingeholt.

Eine Kommune setzte die Videokamera bereits Anfang 2014 außer Betrieb, sie wurde später auf meinen Wunsch abgebaut. Hier waren jedoch wirtschaftliche Aspekte ausschlaggebend. Eine weitere Kommune beabsichtigt, die Videokamera zur Prüfung ihrer weiteren Erforderlichkeit außer Betrieb zu nehmen. Hierbei ist zu beachten, dass das Abschalten der Kamera nicht ausreicht, sondern für Betroffene erkennbar sein muss, dass die Kamera keine Aufnahmen fertigen kann.

Einige Kommunen haben meine Anfrage bis heute nicht beantwortet. Ich habe sie erneut an die Prüfung der bestehenden Videoanlagen erinnert. Eine Veränderung der Anzahl der betriebenen Videoüberwachungsanlagen erwarte ich hierbei jedoch nicht.

Im Rahmen von Beratungsgesprächen oder Prüfungen sind im Zusammenhang mit Videoüberwachungsanlagen einige Punkte aufgefallen, die von allgemeiner Bedeutung sind:

– **Vorsicht beim Updaten oder Überarbeiten von Videoanlagen**
  Bei Prüfbesuchen musste ich mehrfach feststellen, dass nach Wartungsarbeiten vergessen wurde, bereits vorhandene Ausblendungen von Bereichen, die nicht überwacht werden dürfen, wieder einzuschalten. Beim erneuten Anschalten einer Videoanlage müssen deshalb erneut die tatsächlich aufgezeichneten Bilder kontrolliert werden, um unzulässige Aufzeichnungen zu vermeiden.

– **Kennzeichnung der videoüberwachten Bereiche**
  Mittlerweile ist bekannt, dass die gewünschte abschreckende Wirkung einer Videoüberwachungsanlage nur dann erreicht werden kann, wenn auf die Videoüberwachung in ausreichendem Umfang hingewiesen wird. Die Hinweisschilder müssen hierbei so angebracht werden, dass bereits beim Betreten des überwachten Bereichs auf die Überwachung hingewiesen wird. Ein Hinweisschild direkt an der Videoanlage ist regelmäßig nicht ausreichend. Darüber hinaus muss für Betroffene eindeutig erkennbar sein, wer für die Videoüberwachung verantwortlich ist.

– **Dokumentation und Verfahrensverzeichnis**
  Wie erwähnt setzt jede Einrichtung einer Videoüberwachungsanlage voraus, dass vorab überprüft wird, ob alle Voraussetzungen des § 14 Abs. 4 HSOG erfüllt sind. Dies ist zu dokumentieren. Darüber hinaus muss für jede Videoanlage ein Verfahrensverzeichnis erstellt werden. Hierbei müssen Zweck der Videoüberwachung, der überwachte Bereich, Löschfristen und Zugriffsrechte eindeutig beschrieben werden.

4.1.5.8
Einführung von per Funk auslesbaren Wasserzählern

Beim Einsatz von Wasserzählern, die per Funk ausgelesen werden, müssen nicht nur die rechtlichen Rahmenbedingungen geschaffen werden. Die eingesetzte Technik muss auch bestimmte Anforderungen erfüllen.

Im letzten Jahr haben mehrere kommunale Wasserwerke nachgefragt, welche Rahmenbedingungen beim Einsatz von per Funk auslesbaren Wasser-

zählern zu beachten sind. Ausgangslage war, dass Wasserzähler ausgetauscht werden mussten und die Wasserwerke überlegten, wie sie die Möglichkeiten der neuen Technik nutzen können. So kann das Personal mit einem entsprechend ausgestatteten Lesegerät die Wasserstände auslesen, ohne dass jemand in der Wohnung bzw. dem Haus anwesend sein muss. Der Auslesevorgang als solcher ist also mit weniger organisatorischem und zeitlichem Aufwand verbunden.

Da Wasserwerke nicht im Wettbewerb stehen, gilt für die kommunalen Wasserwerke das HDSG ohne Einschränkungen. Insbesondere muss der § 36 HDSG beachtet werden.

§ 36 HDSG

Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in den Geschäftsräumen, ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

Bei meinen Beratungen habe ich auf die dort geforderte Einwilligung hingewiesen. Seitens der Wasserwerke wurden erhebliche Bedenken geäußert, ob von allen Kunden eine wirksame Einwilligung eingeholt werden kann. Falls aber bei einigen Kunden weiterhin „konventionell“ die Zählerstände erhoben werden müssten, würde daraus ein erheblicher Aufwand entstehen.

Vor diesem Hintergrund habe ich auf eine mögliche Lösung hingewiesen, bei der durch eine kommunale Satzung die Einführung von Funk-Wasserzählern beschlossen wird und somit eine Rechtsgrundlage für ihren Einsatz geschaffen wird.

Als Rechtsgrundlage kommt auch eine kommunale Satzung in Betracht. Nach der so genannten Wesentlichkeitstheorie hat der parlamentarische Gesetzgeber zwar alle grundrechtsrelevanten wesentlichen Regelungen selbst zu treffen. Der Umkehrschluss hieraus besagt aber, dass unwesentliche Regelungen mit geringerer Eingriffsintensität von der Exekutive durch Rechtsverordnung oder Satzung getroffen werden können. Die danach zulässige Satzung muss dann aber besonderen Anforderungen genügen. Sie muss insbesondere klar, eindeutig und bestimmt sein und den Grundsatz der Verhältnismäßigkeit beachten. Satzungen über die per Funk lesbaren Wasserzähler müssen daher die technisch organisatorischen Maßnahmen regeln, die die informationelle Selbstbestimmung der Kunden gewährleisten.

Die Zählernummer mit dem jeweils aktuellen Zählerstand ist über die Verknüpfung mit einer Adresse ein personenbezogenes Datum. Zu den Risiken, die betrachtet werden müssen, gehört ein unbefugtes Auslesen des

Verbrauchs in kurzen Abständen; so könnte ein identischer Zählerstand an mehreren Tagen bedeuten, dass die Bewohner nicht im Haus sind. Es sollte aber auch generell ein unbefugtes Mitlesen der Kommunikation verhindert werden. Befugt sind in diesem Fall die mit der Auslesung beauftragten Personen.

Die für den Einsatz der Funkzähler vorgesehene Technik muss einige Anforderungen an die technische Ausgestaltung erfüllen, damit ein unbefugtes Auslesen des Verbrauchs verhindert wird:

– Die Datenübertragung muss verschlüsselt erfolgen. Üblicherweise werden bei der Produktion der Zähler bereits Schlüsselwerte fest einprogrammiert.
– Es dürfen nur dazu vorgesehene Lesegeräte die Zähler auslesen können.

  Lesegeräte benötigen die zu den Zählern passenden Schlüssel.

  Es müssen kundenspezifische, oder eventuell sogar gerätespezifische, Schlüssel vergeben werden. Dies ist bereits bei der Produktion der Zähler zu beachten.
– Jeder Lesevorgang muss auch bei identischen Zählerständen zu unterschiedlichen Kryptogrammen führen.

Wenn die rechtlichen und technischen Anforderungen erfüllt sind, ist ein datenschutzkonformer Einsatz von Funk-Wasserzählern gegeben. Die kommunalen Wasserwerke habe ich im Rahmen meiner Beratung dabei unterstützt, einen datenschutzgerechten Einsatz der Funk- und Wasserzähler sicherzustellen.

4.1.6
Personalwesen

4.1.6.1
Einsichtsrechte Dritter in die Personalakte

Die Einsichtsrechte Dritter in Personalakten unterliegen strengen Voraussetzungen. Um Beschäftigte aus den Personalabteilungen bei der Wahrung dieser strengen Voraussetzungen zu unterstützen, empfehle ich, hierzu eine Hausregelung zu erlassen.

Immer wieder erhalte ich Anfragen zu dem Thema, wer unter welchen Voraussetzungen das Recht hat, Zugang zu fremden Personalakten zu erhalten. Verschiedentlich habe ich diese Fälle in vergangenen Tätigkeitsberichten beschrieben. So habe ich mich etwa in meinem 22. Tätigkeitsbericht

(Ziff. 10.2) mit der Frage auseinandergesetzt, inwieweit der Frauenbeauftragten Zugang zu Personalakten einzuräumen ist. Im 36. Tätigkeitsbericht (Ziff. 5.10.1) habe ich die gleiche Problematik bezogen auf die Innenrevision behandelt. Nicht in diesen Zusammenhang gehört das Einsichtsrecht der Betroffenen selbst in ihre Personalakte, das ich bereits ausführlich in meinem 32. Tätigkeitsbericht (Ziff. 16.2.1) thematisiert habe.

Insbesondere bei der Beratung von Städten und Gemeinden zu Fragen des Beschäftigtendatenschutzes fällt immer wieder auf, dass der eigentliche Grund der Anfrage an mich nicht so sehr eine Unsicherheit bezüglich der rechtlichen Bewertung ist. Häufig war es vielmehr so, dass sich gerade Personalsachbearbeiterinnen und Personalsachbearbeiter z. B. von Gemeindevertreterinnen und Gemeindevertretern, Gemeindevorständen oder anderen Funktionsträgern unter Druck gesetzt fühlten. Ihr Anliegen ist vielfach, sich von mir ihre Rechtsauffassung bestätigen zu lassen, um dann unzulässigen Begehren auf Einsicht in Personalakten nicht allein entgegentreten zu müssen. Zu dieser Hilfestellung bin ich gerne bereit. Eine Möglichkeit, den Nöten der Mitarbeiter und Mitarbeiterinnen der Personalabteilung zu begegnen, hat mir eine Stadt vorgelegt. Dort hat der für Personal zuständige Amtsleiter eine Verfügung erlassen, in der klar geregelt ist, welche Personen der Stadtverwaltung (Oberbürgermeister, Dezernenten, Amtsleiter etc.) unter welchen Voraussetzungen Zugang zu Personalakten erhalten. Die Verfügung regelt auch, welche Personen in der Verwaltung im Zweifel über die Gewährung von Akteneinsicht oder -auskunft entscheiden und nach welchen Kriterien dies geschieht.

Ich denke, dass hier ein guter Weg gefunden wurde, der allen Seiten Klarheit verschafft und insbesondere denjenigen Personen, die die Personalakten verwalten und deshalb immer wieder Begehrlichkeiten ausgesetzt sind, eine gute Grundlage bietet, mit diesen Begehrlichkeiten umzugehen, ohne dass es zu Unstimmigkeiten kommen muss.

4.1.7
Ausländerbehörden

4.1.7.1
Akteneinsicht in Visumakten bei der Ausländerbehörde

In einem Visumverfahren haben Betroffene auch ein Einsichtsrecht in die bei der zuständigen Ausländerbehörde aufbewahrten Aktenbestandteile. Einer vorherigen Zustimmung der deutschen Vertretung im Ausland bedarf es nicht.

Ich erhalte immer wieder Eingaben, mit denen Betroffene geltend machen, dass ihnen die Einsicht in bestimmte Aktenbestandteile im Visumverfahren von der zuständigen Ausländerbehörde verwehrt wird. Das Akteneinsichtsrecht spielt vor allem in folgenden Sachzusammenhängen eine Rolle:

In bestimmten, in § 31 Abs. 1 Aufenthaltsverordnung genannten Fällen bedürfen die von der jeweiligen deutschen Auslandsvertretung erteilten Visa der vorherigen Zustimmung der zuständigen Ausländerbehörde.

§ 31 Abs. 1 AufenthV

Ein Visum bedarf der vorherigen Zustimmung der für den vorgesehenen Aufenthaltsort zuständigen Ausländerbehörde, wenn

1. *der Ausländer sich zu anderen Zwecken als zur Erwerbstätigkeit oder zur Arbeitsplatzsuche länger als drei Monate im Bundesgebiet aufhalten will,*
2. *der Ausländer im Bundesgebiet*
   a) *eine selbständige Tätigkeit ausüben will,*
   b) *eine Beschäftigung nach § 18 Absatz 4 Satz 2 des Aufenthaltsgesetzes ausüben will oder*
   c) *eine sonstige Beschäftigung ausüben will und wenn er sich entweder bereits zuvor auf der Grundlage einer Aufenthaltserlaubnis, einer Blauen Karte EU, einer Niederlassungserlaubnis, einer Erlaubnis zum Daueraufenthalt-EG, einer Duldung oder einer Aufenthaltsgestattung im Bundesgebiet aufgehalten hat oder wenn gegen ihn aufenthaltsbeendende Maßnahmen erfolgt sind oder*
3. *die Daten des Ausländers nach § 73 Absatz 1 Satz 1 des Aufenthaltsgesetzes an die Sicherheitsbehörden übermittelt werden, soweit das Bundesministerium des Innern die Zustimmungsbedürftigkeit unter Berücksichtigung der aktuellen Sicherheitslage angeordnet hat.*

Für den Visumantragsteller kann es von Interesse sein, nicht nur die seine Person betreffende Akte bei der jeweiligen Auslandsvertretung einzusehen, sondern sich – meist vertreten durch einen Anwalt oder eine sonstige Person seines Vertrauens – über die Gründe einer etwaigen ablehnenden Entscheidung der Ausländerbehörde zu informieren. In einigen Fällen haben Ausländerbehörden diese Akteneinsicht mit der Begründung verwehrt, dass die Auslandsvertretung die „aktenführende Stelle“ sei, es sich bei den bei der Ausländerbehörde aufbewahrten Schriftstücken nur um einen Teil dieser Akte handele und deshalb zumindest die Zustimmung der Auslandsvertretung in die Akteneinsicht eingeholt werden müsse.

Diese Auffassung entspricht nicht der geltenden Rechtslage. Einschlägig ist § 29 VwVfG, da es sich bei der Visumantragsstellung um ein Verwaltungsverfahren im Sinne dieses Gesetzes handelt. Insoweit geht das Akteneinsichtsrecht nach § 29 VwVfG auch dem Akteneinsichtsrecht nach § 18 Abs. 5 HDSG vor.

§ 29 HVwVfG

(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Satz 1 gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung. Soweit nach den §§ 17 und 18 eine Vertretung stattfindet, haben nur die Vertreter Anspruch auf Akteneinsicht.

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

(3) Die Akteneinsicht erfolgt bei der Behörde, die die Akten führt. Im Einzelfall kann die Einsicht auch bei einer anderen Behörde oder bei einer diplomatischen oder berufskonsularischen Vertretung der Bundesrepublik Deutschland im Ausland erfolgen; weitere Ausnahmen kann die Behörde, die die Akten führt, gestatten.

Danach haben Beteiligte am Verwaltungsverfahren das Recht auf Einsicht in die das Verfahren betreffende Akte. Dies kann auch bei einer anderen Behörde erfolgen. Ausgenommen davon sind Entwürfe für Entscheidungen und Arbeiten zu ihrer unmittelbaren Vorbereitung. Bei den bei der Ausländerbehörde aufbewahrten Aktenbestandteilen – also beispielsweise Unterlagen über die Ablehnung oder Zustimmung zur Visumerteilung – handelt es sich nicht um derartige Ausnahmen.

Diese Rechtsauffassung findet sich auch in der allgemeinen Verwaltungsvorschrift der Bundesregierung zum Aufenthaltsgesetz (BRDrucks. 669/09 vom 27. Juli 2009 Ziff. 6.4.6).

Bei der Visumerteilung mit Zustimmung der Ausländerbehörde nach § 31 Absatz 1 AufenthV besteht im Rahmen des allgemeinen Verwaltungsverfahrensrechts und des jeweils anwendbaren Datenschutzrechts ein Akteneinsichtsrecht auch gegenüber der zuständigen Ausländerbehörde. Das Akteneinsichtsrecht bezieht sich in diesem Fall auch auf die von der Auslandsvertretung im Zustimmungsverfahren an die Ausländerbehörde übermittelten Aktenbestandteile; ausgenommen hiervon ist bei Akteneinsicht vor Abschluss des Verfahrens jedoch der interne Entscheidungsvorschlag (Votum) der Auslandsvertretung (vergleiche § 29 Abs. 2 Satz 2 Verwaltungsverfahrensgesetz). Die Ausländerbehörde unterrichtet die Auslandsvertretung unverzüglich von der Gewährung der Akteneinsicht.

Ich habe die betroffenen Ausländerbehörden auf diese Rechtslage hingewiesen. Bestehende Dienstanweisungen wurden entsprechend geändert.

4.1.7.2
Datenerhebung von Ausländerbehörden bei Jobcentern

Es ist datenschutzrechtlich unzulässig, wenn Ausländerbehörden ohne weitere Begründung bei Jobcentern anfragen, ob bestimmte Personen im Arbeitslosengeld II-Bezug („Hartz IV“) stehen.

4.1.7.2.1
Der Anlass

Ein Jobcenter hat mich darüber informiert, dass von der Ausländerbehörde regelmäßig – ohne Begründung und ohne Nennung einer Rechtsgrundlage – Anfragen einträfen, ob namentlich aufgeführte ausländische Personen Grundsicherung für Arbeitsuchende – Arbeitslosengeld II – beziehen würden. Das Jobcenter bat mich um Beratung, unter welchen Voraussetzungen Daten an die Ausländerbehörde übermittelt werden dürfen bzw. unter welchen Voraussetzungen Datenerhebungen seitens des Ausländeramtes beim Jobcenter zulässig sind.

4.1.7.2.2
Datenschutzrechtliche Bewertung

Die speziellen datenschutzrechtlichen Normen im SGB II (Grundsicherung für Arbeitsuchende) sehen eine Übermittlung personenbezogener Daten durch das Jobcenter an die Ausländerbehörde nicht vor (vgl. §§ 50 ff. SGB II).

Ergänzend ist das allgemeine Sozialdatenschutzrecht anzuwenden, das in den §§ 67 ff. SGB X geregelt ist.

Beispielsweise erlaubt § 69 Abs. 1 Nr. 1 SGB X die Übermittlung von Sozialdaten durch das Jobcenter an die Ausländerbehörde, soweit dies zur Erfüllung von Aufgaben des Jobcenters erforderlich ist. Mit diesem Thema habe ich mich bereits ausführlich befasst (41. Tätigkeitsbericht, Ziff. 3.3.5.2.3).

Darum geht es hier aber nicht, sondern um die Frage, inwieweit außerhalb der eigenen Aufgabenwahrnehmung durch das Jobcenter Datenübermittlungen betreffend den Sozialleistungsbezug an die Ausländerbehörde zulässig sind, die deren Aufgabenfeld betreffen. In diesem Kontext ist es unzulässig, wenn Jobcenter ohne Ersuchen der Ausländerbehörde an diese Sozialdaten übermitteln.

Diese Thematik ist in § 71 Abs. 2 Satz 1 Nr. 1a SGB X näher geregelt.

§ 71 Abs. 2 SGB X

Die 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 ...*

In diesem Zusammenhang sehen die von der Bundesregierung mit Zustimmung des Bundesrates erlassenen allgemeinen Verwaltungsvorschriften (Art. 84 Abs. 2 GG) vor, dass die Ausländerbehörde bei einem Ersuchen um Datenübermittlung Folgendes anzugeben hat (Nr. 87.1.1.1):

– die Personalien, die zur Identifizierung des Betroffenen erforderlich sind,
– Aktenzeichen der ersuchten Stelle, soweit bekannt,
– welche Daten sie benötigt,
– für welche Aufgabenerfüllung sie die Daten benötigt, wobei in eindeutigen Fällen die Angabe der Rechtsvorschrift ausreicht und
– aus welchen Gründen die Daten ohne Mitwirkung des Betroffenen erhoben werden.

Vor diesem Hintergrund muss also eine Anfrage der Ausländerbehörde beim Jobcenter nicht nur begründet werden, sondern ein solches Ersuchen ist in den Fällen unzulässig, in denen die Informationen beim Betroffenen selbst erhoben werden können.

Reine Arbeitserleichterungen rechtfertigen noch keine Datenerhebung beim Jobcenter unter Außerachtlassung des Grundsatzes der Direkterhebung beim Betroffenen. Wird die Erhebung mit der Überprüfung der Angaben des Betroffenen gerechtfertigt, müssen konkrete Anhaltspunkte für die Unrichtigkeit der Aussage des Betroffenen vorliegen (Huber, Kommentar zum Aufenthaltsgesetz, § 86, Rn.35 f.).

Diese Rechtslage habe ich dem Jobcenter mitgeteilt.

Das Jobcenter hat mich mittlerweile darüber informiert, dass es mit dem Ausländeramt ein datenschutzkonformes Vorgehen abgestimmt hat.

4.1.8
Schulen, Schulverwaltung, Hochschulen, Archive

4.1.8.1
Bereitstellung von Daten aus der Lehrer- und Schülerdatenbank für die Kirchen in Hessen

Anschrift und Geburtsdatum der Lehrkräfte dürfen nicht an die Kirchen übermittelt werden.

Die Bereitstellung von personenbezogenen Daten aus der Lehrer- und Schülerdatenbank LUSD für die evangelische und katholische Kirche in Hessen über das IT-System LUSDIK ist ein neues Verfahren, welches den Kirchen Online-Abfragen ermöglicht. Rechtliche Grundlage für die Bereitstellung der Daten ist § 8 Abs. 1 Hessisches Schulgesetz und der diese Vorschrift konkretisierende Erlass zur Übermittlung personenbezogener Daten an Schulträger und Kirchen vom 19. Dezember 2008 (ABl. 1/09), welcher den Inhalt der Daten, die aus der LUSD generiert werden, festlegt. Neu ist das Online-Abrufverfahren, welches es den Kirchen ermöglicht, nicht nur einmal jährlich zu einem Stichtag die Daten von evangelischen und katholischen Lehrkräften zu erhalten, sondern zu jedem beliebigen Zeitpunkt auf die eigens hierfür generierten Daten zuzugreifen.

4.1.8.1.1
Ausgangslage

Seit geraumer Zeit beschäftigen sich die Kirchen in Hessen sowie Vertreter des Hessischen Kultusministeriums (HKM) mit dem Thema der Datenlieferung an die Kirchen. Dabei geht es einerseits um reine Statistikdaten, wie z. B. die Anzahl der teilnehmenden Kinder und Jugendlichen am Religionsunterricht und deren Geschlecht, welche vom HKM übermittelt werden. Zum anderen betrifft dies aber auch personenbezogene Daten der Lehrkräfte mit der Befugnis, Religionsunterricht der beiden Konfessionen zu erteilen. Von Interesse hierbei ist neben den Namen der Betroffenen u. a. auch deren dienst- bzw. arbeitsrechtlicher Status oder die Anzahl der erteilten Stunden. Dies dient den Kirchen dazu, Vakanzen festzustellen und ggf. planerisch entgegenzusteuern. Diese Daten wurden den Kirchen vom HKM bislang per CD zugestellt. Allerdings waren die Aufbereitung und Struktur der Informationen nicht so, wie dies die Kirchen aus der Vergangenheit im Rahmen einer papiernen Übermittlung gewohnt waren.

4.1.8.1.2
Für die Übermittlung vorgesehener Datensatz

In dem Erlass zur Übermittlung personenbezogener Daten an Schulträger und Kirchen vom 19. Dezember 2008 werden die zu übermittelnden Daten abschließend aufgezählt.

Religionslehrer:

In Nachfolge der ehemaligen Statistik-Erhebungsbögen „ER“ und „KR“ wird die Zusammenstellung des Unterrichtseinsatzes im Fach Religion für die Lehrkräfte mit Lehrerbefähigung bzw. Unterrichtserlaubnis in diesem Fach den jeweils zuständigen Bistümern der beiden Kirchen übermittelt.

Im Einzelnen gehören dazu folgende Daten:
- *Personalnummer*
- *Name*
- *Dienstbezeichnung*
- *Schule mit Kontaktdaten*
- *Lehrbefähigung/Vollmacht*
- *Angaben zum Beschäftigungsverhältnis*
- *Anzahl der erteilten Stunden Religionsunterricht.*

Verfahren:

Die Auswertungen erfolgen auf Basis des Statistikabrufverfahrens der LUSD durch die HZD. Die Daten werden von dort direkt und nach dem Stand der Technik verschlüsselt den Empfängern übermittelt. Das Verfahren ist mit dem Hessischen Datenschutzbeauftragten abgestimmt.

4.1.8.1.3
Künftig ist ein Online-Zugriff der Kirchen mit reduziertem Datensatz möglich

Die bisherige Datenlieferung an die Kirchen, welche mit verschlüsselten Informationen per CD jeweils zum Stichtag 1. November erfolgte, war in vier Berichte aufgegliedert. Nur der vierte Bericht, in dem die Lehrkräfte für den Religionsunterricht benannt sind, enthält personenbezogene Daten, welche einer datenschutzrechtlichen Bewertung unterliegen. In diesem vierten Bericht wurde bislang über die in dem bereits zitierten Erlass vom 19. Dezember 2008 (ABl. 1/09) festgelegten Inhalte hinaus die Anschrift der Lehrkräfte sowie deren Geburtsdatum an die Kirchen geliefert. Dies ist jedoch durch den Erlass rechtlich nicht abgedeckt. Ebenso wenig liegt das Einverständnis der Betroffenen vor, so dass ich für künftige Datenlieferungen eine strenge Orientierung an den Vorgaben des Erlasses eingefordert habe. Mithin stehen in der Folge davon die beiden genannten Merkmale den Kirchen künftig nicht mehr zur Verfügung.

4.1.8.1.4
Technik des Verfahrens

Zugriff auf die Gesamtheit der Daten haben die Kirchen jeweils für ihre Konfession. Eine Segmentierung in Teildatenbestände z. B. für die jeweiligen Bistümer habe ich nicht für erforderlich gehalten, so dass für jede Konfession ein hessenweiter Zugriff auf den Datenbestand möglich ist. Das Verfahren wird als Abrufverfahren mit Online-Zugriff konzipiert. Vom HKM wird aus der LUSD auf der Grundlage des Erlasses ein Datensatz generiert, welcher in einem gesonderten Verzeichnis auf einem Server der HZD liegt. Ein wie auch immer gearteter, unmittelbarer Zugriff auf die Daten der LUSD ist damit ausgeschlossen. Die Datenübertragung erfolgt verschlüsselt über VPN. Zur Identifizierung und Authentifizierung der Nutzerinnen und Nutzer sollen bei der katholischen Kirche Security-Token zum Einsatz kommen. Bei der evangelischen Kirche ist der Einsatz eines Security-Moduls noch zu klären bzw. verbindlich festzulegen.

4.1.8.2
Nutzung von sozialen Netzwerken durch Lehrkräfte in hessischen Schulen

Facebook, Twitter, Google+ oder WhatsApp sind in der Schule nur mit Einschränkungen durch Lehrkräfte nutzbar. Das Hessische Kultusministerium hat auf meine Forderung zur Erstellung eines Leitfadens reagiert und mit meiner Unterstützung eine „Handreichung" zum Umgang mit sozialen Netzwerken im Wirkungsbereich der Schule erstellt.

4.1.8.2.1
Die Entwicklung zu einer Handreichung

Facebook und Co. erfreuen sich bei Schülerinnen und Schülern sowie den Lehrkräften großer Beliebtheit. So sind nach einer aktuellen Studie des Bundesverbandes BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.) mehr als drei Viertel (78 %) der Internetnutzer in mindestens einem sozialen Netzwerk angemeldet. Die Generation der unter 30-Jährigen nutzt die Netzwerke am häufigsten: 89 % der „Digital Natives" (deutsch: digitale Ureinwohner, also Personen, die mit digitalen Technologien wie z. B. dem Internet aufgewachsen sind) sind täglich in ihren Lieblingsnetzwerken aktiv.

Diese Entwicklung hat vor der Schule nicht halt gemacht. Allerdings stellt sich zu Recht die Frage, ob der Nutzung durch Lehrer in Form eines gene-

rellen Verbots begegnet werden soll, wie dies z. B. in Baden-Württemberg oder Rheinland-Pfalz der Fall ist. Datenschutzrechtliche Probleme ergeben sich vor allem aus der unbeschränkten und nicht kontrollierbaren Verarbeitung der personenbezogenen Daten der Nutzer. Die Schule als staatliche Einrichtung steht besonders in der Pflicht, die Sicherheit der schulischen Kommunikation zu gewährleisten. In Hessen hat man sich für ein differenziertes Modell entschieden, was ich ausdrücklich gefördert habe. Mit der Handreichung soll einerseits den Realitäten im Schulalltag Rechnung getragen werden, andererseits den Lehrkräften aufgezeigt werden, in welchen Bereichen die Nutzung dieser Medien unangebracht bzw. unzulässig ist. In Kernbereichen der Schule wie z. B. der dienstlichen Kommunikation oder der Übermittlung personenbezogener Daten ist die Nutzung untersagt, in anderen Situationen, insbesondere als Teil der schulischen Medienbildung, eine Nutzung im und für den Unterricht gestattet.

4.1.8.2.2
Kernaussagen des Papiers

Mittlerweile ist das Papier im Amtsblatt des Hessischen Kultusministeriums und auch auf meiner Homepage veröffentlicht. Nachfolgend benenne ich einige Kernpunkte der Handreichung, deren Beachtung durch die Lehrkräfte von mir künftig geprüft wird.

4.1.8.2.2.1
Schulinterne Lernplattformen sind zu bevorzugen

Es gilt der Grundsatz, dass schulinterne Lernplattformen der Kommunikation mit sozialen Netzwerken vorzuziehen sind. Die Nutzung sozialer Netzwerke ist unabdingbar verbunden mit der Preisgabe persönlicher Informationen. Auf deren Speicherung und möglicherweise unzulässigen Nutzung z. B. im Rahmen einer nicht autorisierten Verbreitung hat der Anwender kaum einen Einfluss.

4.1.8.2.2.2
Private Kontaktpflege

Von einer privaten Kontaktpflege zwischen Lehrkräften und Schülerinnen und Schülern ist ausdrücklich abzuraten. Dies betrifft insbesondere sog. Freundschaften.

4.1.8.2.2.3
Personenbezogene Daten sind tabu

Personenbezogene Daten und Dokumente dürfen über soziale Netzwerke nicht kommuniziert werden. Vorstellbar wäre allenfalls, dass kurzfristige Terminänderungen bzw. Ortswechsel oder aber Änderungen von schulischem Unterricht (z. B. der Schwimmunterricht fällt aus, dafür trifft sich die Klasse auf dem Sportplatz) über soziale Netzwerke der Klasse durch den Lehrer mitgeteilt werden.

4.1.8.2.2.4
Kein Nutzungszwang

Keine Schülerin und kein Schüler oder deren Eltern dürfen gezwungen werden, sich in soziale Netzwerke zu begeben, weil eine andere Form als die Informationsweitergabe über soziale Netzwerke nicht mehr erfolgt.

4.1.8.2.2.5
Medienbildung

Der sichere und kritische Umgang mit sozialen Netzwerken ist als Teil der schulischen Medienbildung zu betrachten. Im Rahmen dessen ist die Nutzung sozialer Netzwerke gewünscht. Darüber hinaus hat diese sich nach den Prinzipien der Erforderlichkeit und Zweckbestimmung auszurichten. Es gilt der Grundsatz, keine Personendaten durch Lehrkräfte zu kommunizieren.

4.1.8.2.3
Perspektivische Betrachtung

Die Handlungsempfehlungen bzw. Vorgaben sind nicht statisch zu betrachten. Vielmehr müssen sich die Inhalte den gesellschaftlichen und technischen Entwicklungen anpassen. Dabei wird im Einzelnen im Auge zu behalten sein, wie Netzwerke sich auf der einen Seite weiterentwickeln, auf der anderen Seite aber auch von der Bildfläche verschwinden könnten. So hat sich etwa schülerVZ zum 30. April 2013 aus dem Netz verabschiedet und auch studiVZ hat stark rückläufige Nutzerzahlen. Dennoch ist davon auszugehen, dass soziale Netzwerke bis auf weiteres ein wesentliches Instrument der privaten Kommunikation vor allem jüngerer Menschen und damit auch von Schülerinnen und Schülern bleiben. Gerade deshalb bleibt eine fortlaufende datenschutzrechtliche Betrachtung des Mediums unabdingbarer Bestandteil des Arbeitsaufkommens der Aufsichtsbehörden für den Datenschutz.

4.1.8.3
Unzulässige Datenerhebung und Speicherung in einer Schülerakte

Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler an öffentlichen Schulen in Hessen ist die „Verordnung über die Verarbeitung personenbezogener Daten und statistischen Erhebungen an Schulen" vom 4. Februar 2009. In deren Anlage 1 sind abschließend die Grunddaten der Schülerinnen und Schüler aufgeführt, welche Bestandteil der Schülerakte sind. Personenstandsurkunden dürfen nicht angefordert und gespeichert werden.

Die Beschwerde von Eltern, deren Kind zunächst in der Grundschule des Heimatortes eingeschult wurde, nach wenigen Monaten jedoch die Schule wechselte, ließ mich tätig werden. Der Schulleiter der neu aufnehmenden Schule hatte bei der Durchsicht der Schülerakte festgestellt, dass darin Personenstandsurkunden enthalten waren. Er nahm die Dokumente aus der Akte heraus und übergab diese dem erziehungsberechtigten Vater.

In Personenstandsurkunden (im Sprachgebrauch auch als Stammbuchurkunden bezeichnet) werden sehr viel mehr Daten zur Familie und Familienangehörigen erfasst als für die Schule selbst notwendig sind. So enthalten derartige Unterlagen z. B. Angaben zur Scheidung einer Ehe, der Annahme „an Kindes statt" oder aber Angaben zu Familienangehörigen einschließlich des Verwandtschaftsverhältnisses.

Im Zusammenhang mit der Einschulung hat die Schule selbstverständlich das Recht und die Pflicht, Grunddaten der Schülerin oder des Schülers in Erfahrung zu bringen und Informationen darüber zu erheben, wer der Empfänger der schulischen Kommunikation sein darf. Wohin z. B. sollen Elternbriefe verschickt werden oder an wen sind „blaue Briefe" zu adressieren? Nicht alle Familienverhältnisse sind eindeutig und unkompliziert, weil beide Elternteile erziehungsberechtigt sind und sich das Sorgerecht teilen. Im vorliegenden Fall waren die Familienverhältnisse komplizierter, weil das Sorgerecht auf den Vater übergegangen war, da sich die Eltern getrennt hatten. Auch die Mutter des Vaters war involviert. Nach Darstellung der Schulleitung waren bei den Betroffenen mehrfach erfolglos konkrete Informationen zu der Frage angefordert worden, wer der Sorgeberechtigte ist.

Der Einfachheit halber wandte sich die Schulleitung nun an die Meldebehörde der Gemeinde, forderte Personenstandsurkunden an und nahm diese zur Schülerakte.

Unabhängig davon, dass die Datenübermittlung von der Gemeinde an die Schule rechtswidrig war, was den Verantwortlichen dort auch in aller Deutlichkeit mitgeteilt wurde, hätte weder die Anfrage gestellt noch die Spei-

cherung der Daten in der Schülerakte erfolgen dürfen, da die in den Personenstandsurkunden enthaltenen Daten über die in der Verordnung festgelegten Grunddaten hinausgehen.

Anlage 1 Verordnung zur Verarbeitung personenbezogener Daten

Grunddaten der Schülerin oder des Schülers (Auszug):
- *Namen, Namenszusatz der Eltern*
- *Vornamen der Eltern*
- *Anschrift der Eltern*
- *Erziehungsberechtigung*
- *Erziehungsvereinbarungen*

Mit der Schulleiterin und dem Staatlichen Schulamt wurde der Fall eingehend besprochen. Aufgrund der Gespräche gehe ich davon aus, dass die Schulleitung künftig keine Personenstandsurkunden mehr anfordern wird. Von einer formellen Beanstandung habe ich daher gemäß § 27 Abs. 2 HDSG abgesehen.

5. Aufsichtsbehörde nach § 38 BDSG

5.1
Ordnungswidrigkeiten

5.1.1
Überblick zu den Bußgeldverfahren im Berichtsjahr

In diesem Jahr wurden 20 Bußgeldverfahren abgeschlossen. Darunter befanden sich keine herausragenden Fälle.

Auch in diesem Jahr bezog sich die Mehrzahl der zu bearbeiteten Fälle auf einige wenige der in § 43 BDSG normierten Tatbestände: Nichterfüllung von Auskunftsansprüchen an Betroffene und unzulässige Datenübermittlungen.

Nachdem bekannt wurde, dass das Bayrische Landesamt für Datenschutzaufsicht ein nicht unerhebliches Bußgeld verhängt hatte für die Versendung einer Mail mit einem offenen E-Mail-Verteiler, gab es auch bei mir einige Anzeigen und Anfragen zu diesem Thema. Allerdings kam es im Ergebnis in keinem Fall zur Verhängung eines Bußgeldes.

Ein Teil dieser Fälle bezog sich auf die Verwendung offener Verteiler durch öffentliche Stellen. Auch für diese gilt selbstverständlich, dass die mit einer solchen Mail verbundene Übermittlung von Daten an Dritte in der Regel unzulässig ist. Allerdings ist für diese nicht das BDSG, sondern das HDSG anzuwenden. Dieses Gesetz enthält keine entsprechende Bußgeldvorschrift.

Für die durch nicht-öffentliche Stellen versendeten Mails war festzustellen, dass jeweils einzelne Tatbestandsvoraussetzungen des § 43 Abs. 2 Ziff. 1 BDSG nicht erfüllt waren. Soweit es sich bei den verwendeten E-Mail-Adressen um solche von juristischen Personen (z. B. GmbH yyy@ y.de) oder um sogenannte Funktionspostfächer (z. B. Versand@yyy.de) handelte, kommt das BDSG insgesamt nicht zur Anwendung. Bei personenbeziehbaren Adressen (z. B. a.yyy@y.de) ist zunächst zu prüfen, ob es sich dabei wirklich um ein nicht öffentlich zugängliches Datum handelt. Dies ist zumindest dann zu verneinen, wenn durch einfache Recherchen im Internet diese Mail-Adresse zu finden ist. Auch wenn vielen diese Tatsache nicht bewusst ist: Im Internet veröffentlichte Informationen, die nicht durch besondere Maßnahmen für den allgemeinen Zugriff gesperrt sind, gelten als allgemein zugänglich, sodass auch in diesen Fällen der Bußgeldtatbestand nicht verwirklicht ist.

In § 43 Abs. 1 BDSG werden im Wesentlichen die Bußgeldtatbestände zusammengefasst, die Verstöße gegen die formalen Anforderungen des Gesetzes betreffen (z. B. eine nicht rechtzeitig erteilte Auskunft); Abs. 2 umfasst die Verstöße gegen eine materiell fehlerhafte Datenverarbeitung (z. B. eine unzulässige Datenübermittlung).

Bei den im Berichtsjahr abgeschlossenen Fällen lag in 4 Fällen ein Verstoß gegen § 43 Abs. 1 BDSG zugrunde, 16 Fälle bezogen sich auf § 43 Abs. 2 BDSG. 18 Fälle wurden eingestellt, weil der Anwendungsbereich des BDSG nicht betroffen war oder einzelne Tatbestandsvoraussetzungen des § 43 BDSG nicht erfüllt wurden. Es wurden 2 Bußgelder in Höhe von 1.750 EUR verhängt.

5.1.2
Zum Verhältnis von Zwangsgeld und Ordnungswidrigkeitenverfahren

Bei Aufsichtsmaßnahmen nach § 38 BDSG, die bei den Adressaten kein Gehör finden, stellt sich die Frage der Durchsetzung. Im Einzelfall ist dann zu prüfen, ob ein Verwaltungsverfahren oder ein Bußgeldverfahren erfolgversprechender ist.

Die Aufsichtsbehörde trat in diesem Jahr an die Bußgeldstelle verstärkt mit Fällen nichterteilter Auskunft nach §§ 34 Abs. 1 und 38 Abs. 5 BDSG heran, um in diesen Fällen die Verantwortlichen durch Einleitung eines Bußgeldverfahrens dazu zu bewegen, die angeforderte Auskunft zu erteilen.

Verwaltungszwangsverfahren und Ordnungswidrigkeitenverfahren verfolgen unterschiedliche Zielrichtungen.

Das war Anlass, das Verhältnis der beiden Verfahren zueinander näher zu beleuchten.

Das Ordnungswidrigkeitenverfahren dient der repressiven Ahndung von Verstößen. Zweck des Bußgeldverfahrens ist es nicht, einen Ausgleich für sozialethische Schuld herbeizuführen, wie dies im Strafverfahren der Fall ist. Das Bußgeldverfahren ist in erster Linie darauf gerichtet, eine bestimmte Ordnung durchzusetzen. Die Geldbuße ist eine Unrechtsfolge für eine tatbestandmäßige und vorwerfbare Handlung, wie beispielsweise ein Datenschutzverstoß. Sie hat repressiven Charakter und ist ein mit einer Sanktion verbundener und deshalb spürbarer Pflichtenappell an den Betroffenen. Der Betroffene soll dadurch angehalten werden, auch die im Vorfeld des Rechtsgüterschutzes errichteten Ge- und Verbote zu beachten. Kurz, der Betroffene soll angehalten werden, u. a. datenschutzrechtliche Vorschriften einzuhalten. Im Gegensatz zur Strafe ist die Geldbuße eine Pflichtenmahnung und hat keine ins Gewicht fallende Beeinträchtigung des Ansehens zur Folge. Die Geldbuße soll nicht nur den Betroffenen, sondern auch andere dazu anhalten, die gesetzte Ordnung zu beachten. Außerdem dient die Geldbuße der Gewinnabschöpfung (§ 17 Abs. 4 Satz 1 OWiG) und hat die Aufgabe, unlauterem Gewinnstreben bei wirtschaftlichen Betätigungen vorzubeugen. Im Zusammenhang mit Datenschutzverstößen in der Bußgeld-

praxis wird es schwierig sein, einen wirtschaftlichen Vorteil im Rahmen der Bußgeldzumessung zu beziffern, wenn auch der Bußgeldrahmen hierzu jedenfalls genug Raum bietet. Nach § 43 Abs. 3 BDSG kann eine Geldbuße bis zu 50.000 EUR und in Fällen des § 43 Abs. 2 ein Bußgeld von bis zu 300.000 EUR ausgesprochen werden. Wenn der Bußgeldbescheid Rechtskraft erlangt, erfolgt eine Mitteilung an das Gewerbezentralregister (GZR). Eingetragen werden rechtskräftige Bußgeldbescheide, die gegen natürliche und gegen juristische Personen sowie gegen Personengesellschaften (§§ 30, 88 OWiG) gerichtet sind. Sie sind dem Gewerbezentralregister mitzuteilen, sofern die Voraussetzungen des § 149 Abs. 2 Satz 1 Nr. 3 GewO gegeben sind. Die Ordnungswidrigkeit muss bei oder im Zusammenhang mit der Ausübung eines Gewerbes oder dem Betrieb einer sonstigen wirtschaftlichen Unternehmung begangen worden sein. Der Täter ist Inhaber, gesetzlicher Vertreter (§ 9 Abs. 2 Satz 1 Nr. 1 OWiG) oder auch sonst ausdrücklich beauftragter, eigenverantwortlich tätiger Vertreter (§ 9 Abs. 2 Nr. 2 OWiG) und die Geldbuße beträgt mehr als 200 EUR. Das Bußgeldverfahren ist in seiner Wirkung umfassend nachhaltig. Aber der Verstoß gegen den Datenschutz wird dadurch nicht behoben. Eine noch ausstehende Auskunft ist durch ein gezahltes Bußgeld noch nicht erteilt. Hier helfen die Mittel des Verwaltungszwangs weiter.

Die Mittel des Verwaltungszwangs sind Beugemittel. Sie dienen dazu, die Pflicht zur Vornahme einer bestimmten Handlung, Duldung oder Unterlassung durchzusetzen. Das Zwangsgeld (§ 76 HVwVG) kann unabhängig von der Durchführung eines Bußgeldverfahrens angedroht werden. Die Wirkung der Zwangsmittel besteht darin, den Willen des Verantwortlichen durch mittelbaren Zwang zu beugen, um ihn schließlich zur Erfüllung der sich aus dem zu vollstreckenden Verwaltungsakt ergebenden Verhaltenspflicht zu bewegen. Das Verwaltungszwangsverfahren dient nicht als nachträgliche Sanktion für in der Vergangenheit begangene Rechtsverstöße (OVG Bautzen, SächsVBl. 1996, S. 67).

Die Geldbuße gemäß § 90 Abs. 1 OWiG ist eine Sanktion der Verwaltung, durch die eine schuldhafte Zuwiderhandlung geahndet wird. Bei späterer Befolgung des Gesetzesbefehls wird die Geldbuße im Gegensatz zum Zwangsgeld nicht gegenstandslos.

Der Kosten- und Arbeitsaufwand für die Behörde im Verwaltungszwangsverfahren ist im Vergleich zum Bußgeldverfahren relativ identisch.

Fazit, es gibt kein Schwarz oder Weiß. Grundsätzlich kann und letztlich wird zu entscheiden sein, ob man auf Maßnahmen des Verwaltungszwangs zurückgreift oder gleich ein Bußgeldverfahren einleitet. Um eine nichterteilte Auskunft zu erhalten, ist die Durchsetzung mittels Verwaltungszwangs si-

cherlich zielführender. Es mag Fälle geben, in denen allein schon die Anhörung im Bußgeldverfahren den Betroffenen dazu bewegt, die ausstehende Auskunft zu erteilen, aber darauf darf nicht vertraut werden. Dahingegen kann die Androhung eines Zwangsgeldes in Höhe von beispielsweise 5.000 EUR bereits Wunder wirken und den Verantwortlichen dazu anhalten, seinen Verpflichtungen nachzukommen.

5.1.3
Warum werden Bußgeldverfahren – auch bei festgestellten Verstößen gegen das BDSG – eingestellt?

Im Berichtsjahr wurde im Bußgeldverfahren vermehrt von der Möglichkeit, von einer Ahndung mit einem Bußgeld abzusehen, Gebrauch gemacht.

Oft wird angenommen, eine Ordnungswidrigkeit müsse, so wie die Straftat im Strafverfahren, zwingend verfolgt werden. Dem ist aber nicht so.

Das Bußgeldverfahren untersteht von Anfang bis zum Ende dem Opportunitätsprinzip. Im Gegensatz zum Strafverfahren, das dem Legalitätsprinzip (§ 152 Abs. 2 StPO) unterliegt, besteht im Bußgeldverfahren gerade kein Verfolgungszwang, d. h., eine Ordnungswidrigkeit kann, muss aber nicht geahndet werden.

> *§ 152 StPO*
>
> *(1) Zur Erhebung der öffentlichen Klage ist die Staatsanwaltschaft berufen.*
>
> *(2) Sie ist, soweit nicht gesetzlich ein anderes bestimmt ist, verpflichtet, wegen aller verfolgbaren Straftaten einzuschreiten, sofern zureichende tatsächliche Anhaltspunkte vorliegen.*

Gemäß § 47 Abs. 1 Satz 1 OWiG liegt die Verfolgung von Ordnungswidrigkeiten im pflichtgemäßen Ermessen der Verfolgungsbehörde. Das bedeutet, dass die Bußgeldbehörde darüber entscheidet, ob ein Bußgeldverfahren eingeleitet und durchgeführt wird.

> *§ 47 Abs. 1 Satz 1 OWiG*
>
> *Die Verfolgung von Ordnungswidrigkeiten liegt im pflichtgemäßen Ermessen der Verfolgungsbehörde. Solange das Verfahren bei ihr anhängig ist, kann sie es einstellen.*

Der sachliche Grund für die Anwendung des Opportunitätsprinzips liegt darin, dass Ordnungswidrigkeiten die Rechtsordnung weniger gefährden und einen geringeren Unrechtsgehalt aufweisen als Straftaten. Es ist nach einem angemessenen Verhältnis zwischen der erstrebten Zielrichtung (Ver-

besserung der Einhaltung der Datenschutzvorschriften) und dem Einsatz der Geldbuße zu suchen. Der mit der Geldbuße vorwiegend verfolgte Zweck, eine bestimmte Ordnung durchzusetzen, lässt sich mitunter schon in anderer Weise als mit einer Geldbuße, etwa mit einer Verwarnung oder zum Beispiel mit der Androhung der Verfolgung eines wiederholten Verstoßes oder durch eine beschränkte, aber gezielte Verfolgung bestimmter Verstöße, erreichen. Es geht nicht darum, eine Tat zu „sühnen". Vielmehr geht es darum, präventiv die Einhaltung der Rechtsordnung sicherzustellen.

An den §§ 43 und 44 BDSG wird die Unterscheidung deutlicher. Die in § 43 Abs. 1 und 2 BDSG enthaltenen Tatbestände sind Bußgeldtatbestände. § 44 BDSG sanktioniert die Bußgeldtatbestände in § 43 Abs. 2 BDSG aber als Straftatbestände, wenn bestimmte Voraussetzungen hinzukommen, d. h. wenn die Tatbestände des § 43 Abs. 2 BDSG vorsätzlich, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder zu beschädigen, begangen werden. Dann geht es nicht mehr nur darum, präventiv die Einhaltung der Rechtsordnung sicherzustellen, sondern darum, eine Tat zu „sühnen".

§ 44 BDSG

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Findet das Opportunitätsprinzip Anwendung, wird entschieden, „ob", „in welchem Umfang" und „wie" eine Tat verfolgt werden soll.

Zu diesem Zweck wird abgewogen zwischen der Bedeutung der Ordnungswidrigkeit einerseits und der Zweckmäßigkeit der Verfolgung andererseits. Dabei ist vor allem der Grundsatz der Verhältnismäßigkeit zu beachten. Die Bußgeldstelle muss prüfen, ob die Verfolgung der Tat geeignet ist, das Ziel, die Einhaltung des Datenschutzes zu erreichen, zu fördern oder zu beeinträchtigen und ob der Einsatz der Mittel dazu in einem angemessenen Verhältnis steht.

Ausschlaggebend sind allein sachliche Umstände. Bei der Abwägung sind sämtliche Umstände des Falls zu würdigen. Darunter fallen die Bedeutung und Auswirkung der Tat, der Grad der Vorwerfbarkeit, die Gefahr einer Wiederholung durch andere, die Häufigkeit gleichartiger Verstöße, die Einstellung des Täters zur Rechtsordnung sowie sein Verhalten nach der Tat.

Wird beispielsweise bei einer Firma ein Datenschutzverstoß durch die Aufsicht festgestellt und die Firma ändert aber daraufhin ihre Praxis und ergreift gezielt Maßnahmen, um in Zukunft Datenschutzverstöße dieser Art zu vermeiden, und entsteht beim Dritten kein Schaden, dann kann im Einzelfall die Feststellung des Verstoßes durch die Aufsichtsbehörde ausreichend sein und die Bußgeldstelle von einer Ahndung im Bußgeldverfahren absehen. Anders zu bewerten wäre der Sachverhalt beispielsweise, wenn dieselbe Firma nicht nur einmal wegen eines Datenschutzverstoßes auffällig ist und erkennen lässt, dass der Datenschutz nicht in die strategischen Überlegungen einfließt.

Wäre die Verfolgung einer Tat im Verhältnis zur Bedeutung des einzelnen Verstoßes unverhältnismäßig aufwändig, so kann die Bußgeldstelle im Einzelfall beispielsweise von der Verfolgung absehen.

In jedem Fall handelt es sich um Einzelfallentscheidungen. Die Feststellungen der Aufsichtsbehörde und die Stellungnahme des Betroffenen im Rahmen der Anhörung im Bußgeldverfahren sind hierfür eine wichtige Entscheidungsgrundlage.

5.2.
Querschnitt nicht-öffentlicher Bereich

5.2.1
Videoüberwachung nach Bundesdatenschutzgesetz

„Damit Sie den Überblick behalten“, „Zu Ihrer eigenen Sicherheit wird dieses Gebäude videoüberwacht“ – „Mittels Wildkamera stets im Blick, wann das Schwarzwild zur Kirrung kommt“ – vermeintliche (gute?) Gründe zur Installation von Videoüberwachungskameras gibt es viele. Leider verlieren die Hersteller der Produkte, Händler und nicht zuletzt die Kamerabetreiber bei Vertrieb und Installation der Anlagen allzu oft gesetzliche Bestimmungen aus den Augen.

5.2.1.1
Allgemeines

Wie bereits in meinem 42. Tätigkeitsbericht (Ziff. 4.2.2) prognostiziert, führten auch in diesem Berichtszeitraum immer günstiger werdende Produkte und gezielte Werbung zu einem weiteren Anstieg der Eingabezahl auf diesem Gebiet. Komplette Videoüberwachungssysteme sind mittlerweile auch für den kleinen Geldbeutel erschwinglich. Der Kunde wählt aus zwischen kabelgebundenen Systemen, W-LAN bzw. IP-Netzwerksystemen oder dem günstigs-

ten Modell, einer täuschend echt aussehenden Kameraattrappe. Der Euphorie erlegen, als „Big Brother“ nun endlich den Nachbarn zu enttarnen, der heimlich seine Abfälle auf fremdem Grund und Boden entsorgt, bei Eis und Schnee nicht mehr auf dem Hochsitz ausharren zu müssen, um den Schwarzwildbestand zu erfahren oder einfach jederzeit nach dem Rechten sehen zu können, werden Überwachungskameras in allen Lebensbereichen oftmals unter Verstoß gegen datenschutzrechtliche Bestimmungen installiert.

In vielen Fällen erreiche ich nach förmlicher Anhörung der für die Videoüberwachung verantwortlichen Stellen (Kamerabetreiber) einen durch Neuausrichtung oder Umpositionierung datenschutzkonformen Betrieb der Überwachungskamera. Oftmals reicht bereits eine geringe Veränderung des Neigungswinkels einer Kamera aus, damit Betroffene unzweifelhaft erkennen können, dass im Fokus einer Überwachungskamera nicht der öffentliche Bereich steht.

Der überwiegende Teil meiner Tätigkeit richtet sich insoweit gegen private Kamerabetreiber, die von ihrem Grundstück aus öffentliche Bereiche, insbesondere Gehwege, Straßen und öffentliche Parkplätze, überwachen. Aber auch Überwachungskameras in Schwimmbädern, Fitnessstudios oder Tankstellen nehmen viele Bürger zum Anlass, sich mit einer Eingabe an mich zu wenden.

Andernfalls wirke ich unter Androhung eines Zwangsgeldes darauf hin, dass die streitgegenständlichen Überwachungskameras entfernt werden.

§ 3 Abs. 7 BDSG

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Nach § 38 Abs. 3 BDSG haben mir die Kamerabetreiber auf mein Verlangen hin die notwendigen Auskünfte zu erteilen. Wichtig sind in diesem Zusammenhang eine Begründung, zu welchem Zweck die Videoüberwachung stattfindet, ob und wie lange Aufzeichnungen gespeichert werden oder reines „Monitoring“ im Rahmen eines verlängerten Auges stattfindet, welche Kameramodelle verwendet und vor allem, welche Bereiche von den Überwachungskameras erfasst werden.

§ 38 Abs. 3 BDSG

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1

Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

Kommen Kamerabetreiber dieser Verpflichtung nicht, nicht vollständig oder nicht rechtzeitig nach, stellt dies eine Ordnungswidrigkeit dar und kann mit einer Geldbuße bis zu 50.000 EUR geahndet werden. Parallel oder losgelöst von einem Ordnungswidrigkeitenverfahren ist die Festsetzung eines Zwangsgeldes bis zu 50.000 EUR zur Durchsetzung der Auskunftsverpflichtung möglich. Hiervon musste ich in Einzelfällen Gebrauch machen.

Positiv lässt sich jedoch feststellen, dass die Zahl der Eingaben zwar auf dem hohen Niveau des Vorjahres geblieben ist, bei vielen speichernden Stellen jedoch nicht zuletzt aufgrund breiter Berichterstattung in den Medien ein Bewusstsein darüber entstanden ist, was datenschutzrechtlich zulässig oder unzulässig ist. Das wahllose Installieren von Überwachungskameras ist ein wenig zurückgegangen, es wurden vermehrt datenschutzrechtlich unbedenkliche Überwachungskameras installiert.

5.2.1.2 Videoüberwachung öffentlich zugänglicher Bereiche durch Privatpersonen

Das BDSG regelt in § 6b die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung).

§ 6b BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. *zur Aufgabenerfüllung öffentlicher Stellen,*
2. *zur Wahrnehmung des Hausrechts oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Öffentlich zugänglich sind Bereiche, die dazu bestimmt sind, von der Allgemeinheit betreten zu werden, z. B. Kaufhäuser, Spielhallen und Spielbanken, Schwimmbäder, Museen, öffentliche Parks, öffentliche Parkplätze, Straßen und Gehwege, die im öffentlichen Eigentum stehen oder der Allgemeinheit gewidmet sind.

Im zurückliegenden Berichtszeitraum richtete sich der Großteil der Eingaben gegen die Kameraüberwachung von öffentlichen Straßen, Gehwegen und Parkplätzen durch Privatpersonen. Hierzu zählen in diesem Zusammenhang auch Gewerbetreibende, Firmen und Vereine.

In diesen Fällen haben die Kamerabetreiber die Überwachungskameras meist zu präventiven Zwecken installiert und berufen sich neben der Wahrnehmung des Hausrechts, § 6b Abs. 1 Nr. 2 BDSG, auch auf ein besonderes berechtigtes Interesse, öffentlich zugängliche Bereiche zu überwachen, § 6b Abs. 1 Nr. 3 BDSG.

Das Hausrecht endet jedoch grundsätzlich an der Grundstücksgrenze. Alles darüber Hinausgehende ist öffentlicher Raum und darf von Privatpersonen nicht überwacht werden.

Sofern sich die Kamerabetreiber auf § 6b Abs. 1 Ziffer 3 BDSG als Zulässigkeitsgrundlage berufen, muss das Bestehen einer Gefährdungslage jedoch substantiiert dargelegt werden können. Obligatorisch ist hier die Nennung von konkreten Vorfällen (Diebstahl, Sachbeschädigung), z. B. durch die Vorlage entsprechender Strafanzeigen (unter Nennung des polizeilichen oder staatsanwaltlichen Aktenzeichens). Eine bloße Behauptung reicht hingegen nicht aus. Das Vorliegen berechtigter Interessen ist zu verneinen, wenn die Videoüberwachung lediglich mit dem Ziel einer allgemeinen abstrakten Gefahrenvorsorge begründet wird („nach dem Rechten sehen“, „zur Abschreckung“, vgl. u. a. Simitis, BDSG, 7. Aufl., § 6b Rdnr. 80).

Bei Wohngebäuden und Wohnanlagen einschließlich Grundstücken, Kellerräumen und Tiefgaragen ist regelmäßig davon auszugehen, dass diese nicht öffentlich zugänglich sind.

Nach § 14 Abs. 3 HSOG obliegt ausschließlich den Polizeibehörden die Videoüberwachung öffentlich zugänglicher Bereiche zur Gefahrenabwehr.

§ 14 Abs. 3 HSOG

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.

5.2.1.3
Videoüberwachung von Grundstücken durch Privatpersonen

Eine Videoüberwachung ist zulässig, wenn ausschließlich das **eigene** Grundstück überwacht wird. Die Überwachungskamera ist erkennbar auf das eigene Grundstück zu richten, muss nach außen hin gut sichtbar sein und darf nicht den Eindruck erwecken, dass öffentlicher Bereich oder Nachbargrundstücke miterfasst sein könnten. Die Beobachtungsbefugnis eines Hausrechtsinhabers und/oder Grundstückseigentümers endet grundsätzlich an der Grundstücksgrenze.

In begründeten Ausnahmefällen billige ich der speichernden Stelle zu, geringe Bereiche des öffentlichen Raums mitzuerfassen, beispielsweise dann, wenn in der Vergangenheit nachweislich erhebliche Schäden an einer Hausfassade durch Graffiti entstanden sind. Hierbei handelt es sich grundsätzlich um Einzelfallentscheidungen.

Die Videoüberwachung eines **Nachbargrundstücks** ist in jedem Fall unzulässig. Bei Zuwiderhandlungen kommen Ansprüche auf Schadensersatz, Schmerzensgeld und Beseitigungsansprüche aufgrund eines unzulässigen Eingriffs in das allgemeine Persönlichkeitsrecht in Betracht. Diese Ansprüche können jedoch ausschließlich von den Betroffenen persönlich auf dem Zivilrechtsweg durchgesetzt werden. Ein Einschreiten liegt nicht in meinem Kompetenzbereich.

Bei der Verwendung von Dome-Kameras wirke ich darauf hin, dass diese sichtbar verkleidet oder umbaut werden, sofern diese so installiert sind, dass öffentlich zugängliche Bereiche erfasst werden könnten.

Auch Kameraattrappen werte ich als Geräte zur Videoüberwachung. Nähere Ausführungen hierzu sind meinem 42. Tätigkeitsbericht (Ziffer 4.2.3) zu entnehmen.

5.2.1.4
Videoüberwachung in Kaufhäusern und Geschäften

Im zurückliegenden Berichtszeitraum haben mich zudem einige Eingaben erreicht, welche die Videoüberwachung in Kaufhäusern und Geschäften zum Gegenstand hatten.

Die verantwortlichen Stellen erklärten in den meisten Fällen, dass die Videoüberwachung zur Ausübung des Hausrechts und – je nach Branche – zum Schutz des Personals und sogar auf Wunsch des Personals erfolge. Unternehmen, die mit hochpreisiger oder gefährlicher Ware handeln (z. B. Juweliere, chemische und biologische Substanzen), haben selbstverständlich ein anderes Sicherungs- und Schutzbedürfnis als der „Tante-Emma-Laden" von nebenan. Dennoch darf auch in diesen Unternehmen die Installation eines Videoüberwachungssystems nur Ultima Ratio sein, insbesondere vor dem Hintergrund des Arbeitnehmerdatenschutzes. Arbeitgeber haben grundsätzlich das Recht und auch die Pflicht, ihr Personal zu schützen, allerdings rechtfertigt dies nicht eine mitunter flächendeckende Videoüberwachung einer Verkaufstheke, wo das Personal permanent im Fokus von Videokameras steht, in Sozialräumen oder dem kompletten Back-Office-Bereich.

In zwei Fällen sah ich mich gezwungen, eine Anordnung nach § 38 Abs. 5 BDSG zur Beseitigung festgestellter Verstöße gegen das BDSG zu treffen. Hierbei handelte es sich zum einen um eine flächendeckende Videoüberwachung des Personals in sämtlichen Geschäftsräumen einer Apotheke, zum anderen um die Videoüberwachung öffentlicher Bereiche (Straße/Gehweg) durch den Inhaber eines Arzneimittelgroßhandels.

§ 38 Abs. 5 BDSG

Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

Daraufhin reichten die verantwortlichen Stellen jeweils Klage gegen diesen Verwaltungsakt bei dem zuständigen Verwaltungsgericht ein. Beide Verfahren sind derzeit noch anhängig.

5.2.1.5
Videoüberwachung durch Tierbeobachtungskameras in hessischen Wäldern

Die Videoüberwachung durch Tierbeobachtungskameras in hessischen Wäldern hatte ich bereits in meinem 41. und 42. Tätigkeitsbericht behandelt, dennoch hielt diesbezüglich auch das darauf folgende mediale Echo viele Jagdausübungsberechtigte nicht davon ab, weiterhin die gut getarnten Spione in Hessens Wäldern zu installieren.

§ 15 Abs. 1 Hessisches Waldgesetz (HWaldG) erlaubt grundsätzlich jedem das Betreten des Waldes, sodass der Wald – selbst in Privateigentum – als öffentlich-zugänglicher Bereich im Sinne des § 6b BDSG zu sehen ist.

§ 15 Abs. 1 HWaldG

Jeder darf Wald zum Zwecke der Erholung nach den Maßgaben von § 14 Abs. 1 Satz 3 und 4 des Bundeswaldgesetzes und der nachfolgenden Abs. 2 bis 4 betreten.

Ein Betretungsverbot besteht grundsätzlich nur für die in § 16 Abs. 1 HWaldG genannten Bereiche.

§ 16 Abs. 1 HWaldG

Vom Betreten des Waldes ausgenommen sind

1. *Verjüngungsflächen,*
2. *Waldflächen und Waldwege, auf denen Holzerntearbeiten und andere gefahrgeneigte Waldarbeiten durchgeführt werden,*
3. *forst- und jagdbetriebliche Einrichtungen.*

Radfahren, Reiten und Fahren mit Kutschen ist auf Rückegassen untersagt.

Eine – nicht abschließende Aufzählung – von Jagdeinrichtungen enthält § 22 Abs. 1 Hessisches Jagdgesetz (HJagdG).

§ 22 Abs. 1 HJagdG

Jagdausübungsberechtigte dürfen auf land- und forstwirtschaftlich genutzten Grundstücken besondere Anlagen wie Jagdhütten, Ansitze oder Wildfütterungen nur mit Einwilligung der Grundstückseigentümer errichten. Der Eigentümer ist zur Einwilligung verpflichtet, wenn ihm die Duldung der Anlage zugemutet werden kann und er eine angemessene Entschädigung erhält, die auf Antrag die Jagdbehörde festsetzt.

Werden an jagd- oder forstwirtschaftlichen Bereichen Tierbeobachtungskameras eingesetzt, sind diese Stellen eindeutig zu kennzeichnen, da nicht jeder Waldbesucher eine Kirrung als jagdliche Einrichtung sofort erkennt und somit nicht unterscheiden kann, ob es sich um öffentlichen oder nicht öffentlichen Bereich handelt. Sehr vorbildlich hat dies ein Jagdpächter aus Mittelhessen umgesetzt.

Steht beispielsweise eine Kirrung im Fokus der Kamera, darf es sich hierbei nur um eine ordnungsgemäß angemeldete Kirrung nach § 30 Abs. 8 Satz 1 HJagdG handeln, welche zu diesem Zeitpunkt auch tatsächlich genutzt wird. Sind mehrere Kirrungen angemeldet, jedoch nicht alle tatsächlich genutzt, so darf an den nicht genutzten Kirrungen eine Kameraüberwachung nicht stattfinden.

§ 30 Abs. 8, Satz 1 HJagdG
Die Fütterung zur Bejagung des Schwarzwildes (Kirrung) mit heimischem Getreide, Mais und Erbsen ist zulässig und der Jagdbehörde anzuzeigen.

Um die Zulässigkeit von Tierbeobachtungskameras überprüfen zu können, sollten Bilder der installierten Kameras angefertigt, deren Standort notiert (idealerweise unter Angabe der Koordinaten) und diese Angaben an das zuständige Forstamt oder mich weitergeleitet werden.

5.2.1.6
Videoüberwachung in Frankfurt am Main – Masseneingabe der Bürgerrechtsgruppe „*die*Datenschützer Rhein Main“ vom 26. Mai 2014

Am 26. Mai 2014 erreichte mich eine Eingabe der Bürgerrechtsgruppe „*die*Datenschützer Rhein Main“. Darin sind in tabellarischer Form 369 Standorte von Videokameras im Stadtgebiet Frankfurt am Main aufgelistet, welche öffentlichen Raum überwachen sollen.

Die Bürgerrechtsgruppe „*die*Datenschützer Rhein Main“ hat im Vorfeld bereits selbstständig einige Kamerabetreiber kontaktiert und auf etwaige Gesetzesverstöße hingewiesen. In einigen Fällen konnte sie so einen datenschutzkonformen Betrieb der Videoüberwachungsanlagen erreichen.

Die Fälle, in denen dies nicht möglich war, wurden mir am 26. Mai 2014 zusammengefasst überreicht. Beigefügt waren Bilder der einzelnen Kamerastandorte.

Ich habe umgehend damit begonnen, gegen die verantwortlichen Stellen jeweils ein aufsichtsbehördliches Prüfungsverfahren einzuleiten. Dies stellt sich jedoch mitunter als sehr schwierig dar, da allein bei 93 Positionen Angaben zur speichernden Stelle fehlen, bei 192 Positionen zur speichernden Stelle nur Vermutungen geäußert werden und auch die beigefügten Bilder keine Rückschlüsse auf Kameraausrichtung und Umgebung zulassen, da lediglich die Überwachungskameras selbst auf den Bildern zu sehen sind.

Daher muss von meiner Seite aus zunächst bei Einwohnermeldeämtern, den Kataster- oder Gewerbeämtern die speichernde Stelle recherchiert werden, welche in vielen Fällen, gerade in der Frankfurter Innenstadt, nicht mit dem Grundstückseigentümer identisch ist.

In den bislang eingeleiteten Verfahren konnte jedoch in nicht wenigen Fällen festgestellt werden, dass Überwachungskameras öffentlichen Bereich gerade nicht erfassen und auch der Einstell- bzw. Neigungswinkel dieser Überwachungskameras datenschutzrechtlich zulässig gewählt wurde.

In den übrigen Fällen konnte bislang in Zusammenarbeit mit den speichernden Stellen eine datenschutzkonforme Lösung gefunden werden.

5.2.2
Internationale Aktion zur Prüfung von Apps (GPEN Privacy Sweep)

Wie schon im Jahr 2013 hat meine Behörde auch in diesem Berichtszeitraum wieder am Privacy Sweep des Global Privacy Enforcement Networks (GPEN) teilgenommen. Bei der gemeinsamen Aktion internationaler Datenschutzbehörden wurde diesmal untersucht, ob die Anbieter von Apps den Nutzern ausreichende Datenschutzinformationen zur Verfügung stellen. Lei-

der zeigte sich dabei, dass nur wenige Apps Informationen im erforderlichen Umfang bieten.

Die Nutzung von Apps auf dem Smartphone oder Tablet ist für viele Menschen längst selbstverständlicher Teil des Alltags geworden. Mit Apps werden jedoch häufig eine Vielzahl von – teilweise sehr sensiblen – personenbezogenen Daten erhoben und online an den Anbieter der App oder sogar an Dritte versendet. Nicht wenige Smartphone-Nutzer legen deshalb großen Wert auf einen sparsamen und seriösen Umgang mit ihren Daten und sind zu Recht misstrauisch gegenüber solchen Apps, die mittels verschiedener Systemberechtigungen Daten sammeln, ohne zu erläutern, wozu diese jeweils erforderlich sind. Eine auch aus Datenschutzaspekten bewusste Entscheidung für oder gegen die Nutzung einer App können Nutzer aber nur treffen, wenn sie ausreichend und wahrheitsgemäß über die Verarbeitung von Daten durch die App informiert werden.

Nach § 13 Abs. 1 TMG sind die Anbieter von Apps – genauso wie die Anbieter von Webseiten oder sonstigen Online-Angeboten – gesetzlich dazu verpflichtet, die Nutzer über die Datenverarbeitung bei der Nutzung der App zu informieren.

> *§ 13 Abs. 1 TMG*
>
> *Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten [...] in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.*

Um der Frage auf den Grund zu gehen, wie transparent Apps beim Thema Datenschutz wirklich sind, hat meine Behörde beim diesjährigen GPEN Privacy Sweep gemeinsam mit 25 anderen Datenschutzbehörden aus weltweit 19 Ländern insgesamt über 1.200 Apps untersucht. Das Global Privacy Enforcement Network, das die Aktion koordiniert hat, ist ein informeller Zusammenschluss von Datenschutzaufsichtsbehörden aus der ganzen Welt, der die internationale Zusammenarbeit von Datenschutzbehörden fördert. Im Rahmen der Aktion haben meine Mitarbeiter eine repräsentative Auswahl von Apps hessischer Anbieter und Entwickler für die gängigsten Smartphone-Betriebssysteme iOS und Android untersucht. Die Apps wurden daraufhin überprüft, ob die Nutzer vor der Installation und in der App in ausreichendem Maße über die Datenerhebung und -verarbeitung informiert werden. Bei der Prüfung wurde zudem ein besonderer Fokus auf einige Apps

einer hessischen gesetzlichen Krankenkasse gelegt. Diese wurden zusätzlich daraufhin überprüft, ob sie möglicherweise sensible Gesundheitsdaten ohne Kenntnis der Nutzer erheben.

Im Gegensatz zum letztjährigen GPEN Sweep, bei dem die Datenschutzerklärungen von klassischen Webseiten mit weitgehend positiven Ergebnissen analysiert wurden, fielen die Ergebnisse der diesjährigen Überprüfung von Apps leider ernüchternd aus. Sie zeigten, dass sich viele Anbieter und Entwickler von Apps der für sie geltenden datenschutzrechtlichen Anforderungen scheinbar nicht bewusst sind. Lediglich einige wenige positive Beispiele fielen auf. Dies waren meist Apps größerer Unternehmen oder staatlicher Stellen, die den datenschutzrechtlichen Anforderungen zumindest weitgehend entsprachen. Die meisten untersuchten Apps zeigten dagegen erhebliche Defizite beim Inhalt der Datenschutzerklärung, sofern es eine solche überhaupt gab. Damit entsprach das Ergebnis aus Hessen leider auch den Erfahrungen, die die anderen teilnehmenden Datenschutzbehörden weltweit mit den von ihnen untersuchten Apps gemacht haben.

So war beispielsweise häufig zu beobachten, dass notwendige Informationen nicht schon vor der Installation der App im Online-Store bereitgestellt wurden, sondern erst in der App selbst abgerufen werden konnten. Zu diesem Zeitpunkt wurden aber häufig bereits Daten erhoben und verarbeitet. Bei einigen Apps fanden sich sogar gar keine Datenschutzhinweise oder es wurde auf irrelevante Texte zu anderen Dienstleistungen des Anbieters verlinkt. Auch die vorhandenen Datenschutzhinweise waren häufig inhaltlich unvollständig. So erfordern beispielsweise fast alle Apps den Zugriff auf bestimmte, vom Betriebssystem vorgegebene Systemberechtigungen zur Nutzung von im Gerät gespeicherten Daten und zur Betätigung der Sensoren des Smartphones. Trotzdem erläutern nur die wenigsten Apps, wozu dies jeweils notwendig ist und wofür die so gesammelten oder erzeugten Daten benötigt werden. Auf diese Weise lässt ein Großteil der untersuchten Apps die Nutzer im Unklaren darüber, welche Daten genau zu welchen Zwecken erhoben und verarbeitet werden. Bei manchen Apps lässt dies sogar den Verdacht zu, dass bestimmte Daten gar nicht für die eigentlichen Zwecke der App erhoben werden, sondern dass mittels der App unzulässigerweise und unbemerkt von den Nutzern Daten gesammelt werden sollen.

Auch bei den untersuchten Krankenkassen-Apps zeigten sich teilweise Mängel bei den Datenschutzhinweisen. Allerdings konnte erfreulicherweise durch eine eingehende technische Untersuchung festgestellt werden, dass durch die Apps keinerlei Gesundheitsdaten der Nutzer an die Krankenkasse oder an Dritte übermittelt werden.

Bei der Nachbereitung der Aktion habe ich, ebenso wie viele der an der Aktion beteiligten internationalen Kollegen, die Anbieter und Entwickler der negativ aufgefallenen Apps aus meinem Zuständigkeitsbereich angeschrieben und gefordert, dass die festgestellten Verstöße abgestellt werden und die Datenverarbeitung durch die Apps für die Nutzer transparenter wird. Durch den internationalen Charakter der Aktion und die Vielzahl der überprüften Apps besteht die Hoffnung, dass zumindest bei einigen Anbietern und Entwicklern ein Bewusstsein für die Bedeutung des Datenschutzes bei Apps geweckt wird.

5.3
Kreditinstitute, Auskunfteien und Inkassounternehmen

5.3.1
Datenabfrage mittels Pflichtfeld bei Kreditkartenantrag sowie SCHUFA-Anfrage

Bei einem (Online-)Antrag auf Abschluss eines Kreditkartenvertrags dürfen mittels eines Pflichtfeldes ausschließlich Daten erhoben werden, die für den Antrag notwendig sind. Eine Bonitätsanfrage an Auskunfteien darf erst erfolgen, wenn der Antrag vollständig gestellt worden ist.

Im Rahmen der datenschutzrechtlichen Prüfung eines Sachverhalts ist mir zur Kenntnis gelangt, dass ein Kreditkartenunternehmen im Rahmen eines Online-Antrags auf Abschluss eines Kreditkartenvertrags u. a. folgende Daten mit Hilfe eines Pflichtfeldes erhoben hat:

- Daten zum Beschäftigungsverhältnis
- Firmenname
- Anschrift
- Telefonnummer beider Arbeitgeber
- Position im Unternehmen

Zusätzlich wurde festgestellt, dass bereits vor vollständiger Antragstellung eine Bonitätsanfrage an eine Auskunftei gestellt wurde.

Nach § 4 Abs. 1 BDSG ist u. a. eine Erhebung von Daten nur dann zulässig, wenn dies durch ein Gesetz oder eine andere Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat.

§ 4 Abs. 1 BDSG

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Erhebung der personenbezogenen Daten wie Name, Anschrift, Geburtsdatum, Einkommenssituation ist daher bei der gewählten Produktvariante nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG mittels Pflichtfeld zulässig, da diese Daten für den Abschluss des Vertrags mit dem Betroffenen erforderlich sind. Beispielhaft sei hier die Identifizierungspflicht nach dem Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) genannt.

§ 28 Abs. 1 Nr. 1 BDSG

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. *wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,*

...

§ 3 Abs. 1 Nr. 1 GwG

(1) Verpflichtete im Sinne von § 2 Abs. 1 haben in den in Absatz 2 genannten Fällen die nachfolgenden allgemeinen Sorgfaltspflichten zu erfüllen:

1. *die Identifizierung des Vertragspartners nach Maßgabe des § 4 Abs. 3 und 4,*

...

Für die eingangs genannten Daten hingegen ist eine Erhebung über ein Pflichtfeld unzulässig. Das Unternehmen argumentierte zwar damit, dass die Angaben zu dem Beschäftigungsverhältnis notwendig seien, da bei vermuteten oder tatsächlichen Betrugs- und Missbrauchsfällen so die Karteninhaber zeitnah kontaktiert werden könnten. Diese Argumentation überzeugt allerdings nicht. So ist es einerseits möglich, die Betroffenen auf anderem Wege zu kontaktieren, andererseits kann es für die Karteninhaber durchaus arbeitsrechtliche Konsequenzen haben, wenn sie während der Arbeitszeit private Telefongespräche führen oder ihnen gar private Post an die Firmenanschrift gesandt wird.

Eine freiwillige Preisgabe der Daten durch die Antragsteller hingegen ist durch mich nicht zu kritisieren, da die Erhebung dann auf Grundlage einer Einwilligung im Sinne des § 4a BDSG erfolgt.

§ 4a Abs. 1 BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Vor diesem Hintergrund hat das Unternehmen die dargestellte Praxis der Datenerhebung mittels Pflichtfeld nach meiner Aufforderung eingestellt.

Ebenfalls beanstandet werden musste das Verfahren der Bonitätsabfrage im Rahmen des Antrags auf Abschluss eines Kreditkartenvertrags.

Eine Bonitätsabfrage bei einer Auskunftei darf nach § 28 Abs. 1 Nr. 2 BDSG vorgenommen werden, sofern es zur Wahrung des berechtigten Interesses des Unternehmens erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen überwiegt.

Ein berechtigtes Interesse des Unternehmens an der Kenntnis der Bonitätsdaten der Betroffenen kann damit begründet werden, dass ein Kreditkartenvertrag mit einem potenziellen finanziellen Risiko für das Unternehmen einhergeht, so dass vor Annahme des Antrags die finanzielle Situation der Betroffenen überprüft werden muss.

Die Beantragung der Kreditkarte durch die Betroffenen erfolgte im ersten Schritt online auf dem Internetauftritt des Unternehmens. Über die allgemeinen Informationen zur Kreditkarte wurden die Betroffenen zu dem Antrag auf Abschluss eines Kreditkartenvertrags weitergeleitet.

So wies das Kreditkartenunternehmen im Rahmen des Online-Antrags im Anschluss an die Bestätigung des Buttons „Jetzt beantragen“ darauf hin, dass die Antragsbearbeitung eine SCHUFA-Anfrage beinhalten würde.

Nach Eingabe der personenbezogenen Angaben musste den Mitgliedschaftsbedingungen zugestimmt werden, die unter anderem die sogenannte SCHUFA-Klausel, also die Zustimmung zur Übermittlung der personenbezogenen Daten an die SCHUFA, beinhaltete.

Nach erfolgter Zustimmung konnte der Antrag online abgesendet werden, woraufhin die SCHUFA-Bonitätsanfrage veranlasst wurde.

In den von den Betroffenen akzeptierten Mitgliedschaftsbedingungen war aber der Vertragsabschluss wie folgt geregelt:

„Mit dem Ausfüllen und Unterzeichnen des Antrags auf Ausstellung der Karte geben Sie ein verbindliches Angebot auf Abschluss des Kreditkartenvertrages ab …“

Ein Antrag auf Abschluss des Kreditkartenvertrags kam daher erst mit Unterschrift des Betroffenen zustande. Insofern lagen die rechtlichen Voraussetzungen des § 28 Abs. 1 Nr. 2 BDSG für die Abfrage von Bonitätsdaten bei der SCHUFA nicht vor, da aufgrund der fehlenden Unterschrift faktisch noch kein Antrag auf Abschluss eines Kreditkartenvertrages gestellt worden war.

Auch in diesem Punkt hat das Unternehmen nach meiner Intervention die rechtswidrige Praxis eingestellt.

5.3.2
Zugriffsberechtigungen bei Kreditinstituten

Eine Prüfung mehrerer großer hessischer Kreditinstitute hat ergeben, dass diese angemessene Maßnahmen treffen, um zu verhindern, dass ihre Mitarbeiter ohne ausreichende Berechtigung auf die Daten der Bankkunden zugreifen.

Grundsätzlich ist der Zugriff auf personenbezogene Daten, und damit auch der Zugriff auf Kundendaten durch Mitarbeiter von Kreditinstituten, so weit wie möglich zu beschränken. So dürfen gerade auf die besonders sensiblen Daten von Bankkunden nur diejenigen Bankmitarbeiter zugreifen, die diese Daten benötigen, weil sie für den jeweiligen Kunden tätig werden. In jedem Einzelfall (z. B. Bearbeitung eines Kundenwunsches am Serviceschalter) dürfen Kundendaten nur durch den jeweils zuständigen Mitarbeiter genutzt werden, wenn dies nach den §§ 27 ff. BDSG bzw. spezialgesetzlichen Erlaubnisnormen zulässig ist.

Viele Kunden von regional oder bundesweit tätigen Filialbanken erwarten, dass sie – neben dem Online- und Telefonbanking – auch in jeder Filiale des Kreditinstituts Bankgeschäfte vornehmen können. Um dies zu ermöglichen, muss das Kreditinstitut aber einem großen Teil seiner in der Kundenbetreuung tätigen Mitarbeiter die Möglichkeit geben, im Computersystem des Instituts auf die Daten (fast) aller Kunden zugreifen zu können. Bei großen Kreditinstituten hat dies zur Folge, dass teilweise mehrere tausend Mitarbeiter auf die Daten der Bankkunden zugreifen können.

Um zu verhindern, dass diese Zugriffsmöglichkeiten von den Bankmitarbeitern zu privaten Zwecken oder gar zur Befriedigung der Neugier ausgenutzt werden, sind die Kreditinstitute gem. § 9 S. 1 BDSG i. V. m. S. 2 Nr. 3

der Anlage zu § 9 S. 1 BDSG dazu verpflichtet, Maßnahmen zu ergreifen, die einen Missbrauch der Kundendaten effektiv verhindern.

§ 9 BDSG

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Anlage zu § 9 S. 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

...

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) ...

Im Berichtszeitraum habe ich bei mehreren großen Kreditinstituten mit Sitz in Hessen die Existenz und Wirkung solcher Maßnahmen überprüft.

Alle geprüften Kreditinstitute haben ein gut organisiertes und auf den jeweiligen Geschäftsbetrieb zugeschnittenes Zugriffsberechtigungssystem, nach dem Zugriffsrechte nur an solche Mitarbeiter vergeben werden, die diese auch für ihre jeweilige Aufgabe benötigen. Dabei erhält nicht jeder Mitarbeiter Zugriffsrechte auf alle verfügbaren Kundendaten, sondern nur auf diejenigen Daten, die er für seine Tätigkeit benötigt. So genügt z. B. für viele Aufgaben ein Überblick über den aktuellen Kontostand, ohne dass die einzelnen Buchungen eingesehen werden müssten. Soweit die Zugriffsrechte einzelner Mitarbeitergruppen sehr umfassend sind, konnte dies stets begründet werden, da die jeweiligen Aufgaben der Mitarbeiter solche weitgehenden Rechte erfordern. Zudem bieten manche Kreditinstitute besondere Konten z. B. für VIP-Kunden an, bei denen nur wenige Mitarbeiter Zugriff auf die Kundendaten haben. Bei solchen Angeboten kann jedoch der Service der Bank nicht in vollem Umfang genutzt werden.

Um trotz der teilweise weit reichenden Zugriffsrechte Missbrauch wirksam zu verhindern, ist die Protokollierung aller Zugriffe auf Kundendaten erfor-

derlich. Auf diese Weise können die Einhaltung der bestehenden Zugriffsbeschränkungen überprüft und eventuelle Missbrauchsfälle nachträglich aufgeklärt werden. Sämtliche angefragten Kreditinstitute gaben an, dass sie die Zugriffe auf Kundendaten in ihrem System automatisch protokollieren. Die Protokolldaten werden dabei sicher verwahrt, nach angemessener Zeit wieder gelöscht und können nur von einem eingeschränkten Personenkreis eingesehen werden. Überprüfungen der getätigten Datenzugriffe anhand der Protokolldaten finden teilweise im Wege von regelmäßigen Stichproben oder anlassbezogen zur Aufklärung von konkreten Verdachtsfällen statt.

Im Laufe der Überprüfung haben alle geprüften Kreditinstitute nachgewiesen, dass sie – entsprechend ihrer jeweiligen Größe und ihrem Geschäftsmodell – angebrachte und zuverlässige Maßnahmen ergriffen haben, um einen Missbrauch von Kundendaten durch Mitarbeiter zu verhindern.

Nur kurze Zeit nach der Überprüfung zeigte sich, dass sich diese Sicherheitsmaßnahmen auch tatsächlich in der Praxis bewähren: Mich erreichte die Beschwerde einer Bankkundin, dass ihre Kontodaten unberechtigt von einer Bankmitarbeiterin in Erfahrung gebracht worden seien. Die Mitarbeiterin befand sich in einem privaten Rechtsstreit mit der Beschwerdeführerin, die zufällig Kundin der Bank war. Anhand der protokollierten Zugriffsdaten konnte aufgeklärt werden, dass die Bankmitarbeiterin ihre Position und Zugriffsrechte missbraucht hatte, um Informationen über die Beschwerdeführerin und ihre Konten zu erlangen. So ließ sich nachvollziehen, dass die Mitarbeiterin innerhalb eines längeren Zeitraums sehr häufig auf die Daten der Beschwerdeführerin zugegriffen hatte, obwohl es keinen ersichtlichen Grund dafür gab und die Mitarbeiterin nicht in einer Filiale am Wohnort der Beschwerdeführerin arbeitete. Gegen die Mitarbeiterin der Bank wurde ein Bußgeldverfahren eingeleitet, zudem drohen ihr arbeitsrechtliche Konsequenzen.

5.3.3
Aufzeichnung von Telefonaten in Kreditinstituten

Bei einer Prüfung der aktuellen Praxis der Telefonaufzeichnungen von Kreditinstituten habe ich Defizite festgestellt. Ich habe die Anforderungen dargelegt. Die betroffenen Kreditinstitute erfüllen jetzt diese Anforderungen oder bieten gleichwertige Ersatzlösungen an.

Der Kontakt zu Kreditinstituten erfolgt immer häufiger durch elektronische Kommunikationsmittel. Im Bereich des Onlinebankings sind aufgrund der Verwendung von standardisierten Formularen alle Erklärungen in der Regel unmissverständlich. Außerdem können ausgefüllte Formulare oder mittels

Webseiten ausgelöste Vorgänge leicht und umfassend aufgezeichnet werden. Im Gegensatz dazu kann es im Telefonbanking zu Missverständnissen und Nachweisschwierigkeiten kommen.

Dies hat dazu geführt, dass die meisten Kreditinstitute die mit ihnen geführten Telefonate aufzeichnen. Die dafür benötigte Technik ist mittlerweile verfügbar und leicht einzusetzen. Es besteht deshalb das Risiko einer Aufzeichnung von Telefonaten, die über das erlaubte Maß hinausgeht. Um dies zu vermeiden, habe ich die aktuelle Praxis der Telefonaufzeichnung von Kreditinstituten einer Prüfung unterzogen, mich zunächst jedoch auf die Rechte der anrufenden Kunden beschränkt. Dabei habe ich festgestellt, dass eine Neigung zu einer sehr umfassenden Speicherung von Telefonaten besteht, und die allgemeinen Anforderungen an solche Aufzeichnungen skizziert.

5.3.3.1
Rechtsgrundlage der Telefonaufzeichnung

Die telefonische Kommunikation unterliegt dem Fernmeldegeheimnis des § 88 TKG. Diese richtet sich jedoch nur an die Anbieter von Telekommunikationsdiensten. Dazu zählen Kreditinstitute jedenfalls gegenüber ihren Kunden nicht.

Die Verletzung der Vertraulichkeit des Wortes ist aber dennoch nach § 201 StGB mit Strafe bewehrt und daher umfassend geschützt. Nach § 201 StGB ist die unbefugte Aufzeichnung von Telefonaten verboten.

§ 201 StGB

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt
1. *das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder*
2. *eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.*

(2) Ebenso wird bestraft, wer unbefugt
1. *das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder*
2. *das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.*

Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

Dies schließt die Aufzeichnung ohne vorherige Information darüber aus. Eine vorherige Information über die Aufzeichnung schafft jedoch keine ausreichende Rechtsgrundlage für die Aufzeichnung.

Eine Befugnis zur Aufzeichnung ergibt sich auch nicht aus § 28 Abs. 1 Nr. 1 und 2 BDSG. Die Aufzeichnung von Telefonaten mag zwar für ein Kreditinstitut zu Nachweiszwecken nützlich sein. Die Aufzeichnung eines Telefonates ist jedoch weder erforderlich zur Durchführung des am Telefon besprochenen Geschäftes noch zur Wahrung berechtigter Interessen des Kreditinstitutes. Darüber hinaus würden die schutzwürdigen Interessen des Kunden einer Aufzeichnung entgegenstehen. Zusätzlich ist zu Lasten des Kreditinstitutes zu berücksichtigen, dass in aller Regel nicht nur die betreffende Order oder der Geschäftsabschluss aufgezeichnet werden, sondern zusätzliche Gesprächsanteile, die mit dem beabsichtigten Geschäft nicht in direkten Zusammenhang stehen. Eine vollständige Aufzeichnung der gesamten telefonischen Kommunikation lässt sich aus § 28 Abs. 1 BDSG daher in keinem Fall rechtfertigen.

Auch Regelungen zu Aufzeichnungs- und Aufbewahrungspflichten von Kreditinstituten, wie diese in § 25a Abs. 1 S. 6 Nr. 2 KWG, § 34 WpHG, § 14 Abs. 9 WpDVerOV enthalten sind, finden keine Anwendung. Die Aufbewahrungspflichten beziehen sich nicht auf Telefonate, sondern vielmehr auf die Unterlagen, die in der Ausführung des Geschäftes entstanden sind. Auch andere aufsichtsrechtliche Regelungen oder Empfehlungen der Bankenaufsicht enthalten keine Verpflichtung zur Aufzeichnung von Telefonaten mit Endkunden. Derartige Verpflichtungen betreffen allenfalls Handelsgeschäfte zwischen Kreditinstituten.

Ob gesetzliche Regelungen, welche die Gesprächsaufzeichnung von Telefonaten nicht ausdrücklich regeln, überhaupt als Rechtsgrundlage geeignet sind, ist ohnehin zweifelhaft. Die Aufzeichnung von nicht öffentlichen Gesprächen ohne Einwilligung stellt einen Eingriff in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG dar (BVerfG, Beschluss vom 9. Oktober 2002, 1 BvR 1611/96, 1 BvR 805/98, BVerfGE 106, 28-51). Es bedarf daher einer Rechtsgrundlage von gleichem Rang, um einen derartigen Eingriff zu rechtfertigen (BGH, Urteil vom 17. Februar 2010, VIII ZR 70/07, juris RN 28). Die vorstehenden Vorschriften sind daher grundsätzlich nicht geeignet, eine Aufzeichnung von Telefonaten ohne Einwilligung zu rechtfertigen.

Damit bleibt als Rechtsgrundlage für die Aufzeichnung von Telefonaten nur die Einwilligung nach §§ 4 Abs. 1, 4a BDSG.

5.3.3.2
Anforderungen an die Wirksamkeit der Einwilligung

An die Wirksamkeit der datenschutzrechtlichen Einwilligung im Sinne der §§ 4 Abs. 1, 4a BDSG werden hohe Anforderungen gestellt. Insbesondere muss die Einwilligung freiwillig erfolgen, der Betroffene muss hinreichend aufgeklärt und die Einwilligung besonders hervorgehoben werden.

§ 4 BDSG

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. *eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder*
2. *a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder*
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. *die Identität der verantwortlichen Stelle,*
2. *die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und*
3. *die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,*

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a BDSG

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Bei der Einholung einer Einwilligung ist der gesetzliche Grundgedanke der Datensparsamkeit aus § 3a BDSG und der Erforderlichkeit aus § 28 Abs. 1 BDSG zu beachten. Weder der Umfang der Einwilligung noch deren spätere Umsetzung dürfen diese gesetzlichen Grundgedanken vollständig aufheben. Ein von der Einwilligung unterstütztes Kommunikations- und Aufzeichnungskonzept muss daher grundsätzlich zwischen aufzuzeichnenden und nicht aufzuzeichnenden Gesprächen unterscheiden. Telefonate und Inhalte, deren Aufzeichnung sich aus dem Geschäftsmodell nicht begründen lässt, dürften deshalb nicht aufgezeichnet werden. Das Gleiche gilt für Gespräche, bei denen eine Aufzeichnung unverhältnismäßig wäre oder die Interessen der Betroffenen verletzt, ohne dass dem berechtigte Interessen des Kreditinstitutes gegenüberstehen. Für Telefonate, die nach diesen Maßstäben nicht aufgezeichnet werden dürfen, muss es Kommunikationskanäle geben, die aufzeichnungsfrei sind.

Unstrittig begründbar erscheint die Aufzeichnung von Gesprächen, die ein Bankgeschäft zum Inhalt haben und die ohnehin dokumentiert werden müssten (z. B. Überweisungen, Wertpapier-Orders, Konditionenvereinbarungen, Auskünfte über Umsätze etc.). Nicht ausreichend begründbar sind dagegen Aufzeichnungen bei Fragen zum Service, Öffnungszeiten, technischen Problemen, die Anforderung von Formularen etc.

Dabei besteht nicht das Erfordernis, im Text der Einwilligung nach dem Inhalt der Gespräche zu unterscheiden oder bei der Aufzeichnung einzelner Gespräche die Erforderlichkeit jeweils einzelfallbezogen zu prüfen. Vielmehr reicht es aus, wenn eine Infrastruktur oder Prozesse zur Verfügung gestellt werden, die eine Unterscheidung zwischen aufzuzeichnenden Gesprächen und nicht aufzuzeichnenden Gesprächen ermöglichen. Dieser kann sich ein anrufender Kunde dann entsprechend bedienen und damit die Aufzeichnung in Grenzen steuern.

In Einzelfällen, in denen die Aufzeichnung von Telefonaten nur einmalig oder gelegentlich erfolgt, kann es zulässig sein, eine telefonische Einwilligung vor dem eigentlichen Telefonat einzuholen. Zwar ist nach § 4a Abs. 1 Satz 3 BDSG grundsätzlich Schriftform für die Einwilligung vorgeschrieben. Bei

einzelnen Anrufen ist jedoch die mündliche Einwilligung als Form angemessen. Zwingend erforderlich wäre hierbei allerdings, dass dem Anrufer die Möglichkeit gegeben wird, der Aufzeichnung zu widersprechen. Dann wäre auch eine Einwilligung in die Aufzeichnung durch das aktive Führen des Telefonates in Kenntnis der Aufzeichnung in Einzelfällen datenschutzrechtlich zulässig.

In Fällen, in denen das Telefon für die Durchführung der Bankgeschäfte erforderlich ist (z. B. Telefonbanking), dauerhaft und nicht nur gelegentlich aufgezeichnet wird oder keine Widerspruchsmöglichkeit besteht, ist hingegen eine schriftliche Einwilligung notwendig. Diese muss im Vorfeld der Aufzeichnung eingeholt werden.

Sofern die Einwilligung als Bestandteil allgemeiner Geschäftsbedingungen (AGB) eingeholt werden soll, muss diese gem. § 4a Abs. 1 Satz 4 BDSG besonders hervorgehoben dargestellt werden. Dies verbietet es, eine Einwilligung zur Aufzeichnung von Telefonaten in den hinteren Ziffern der AGB an bereits bestehende AGB anzuhängen.

Zusätzlich müssen erteilte Einwilligungen auch zivilrechtlich wirksam sein. Sie stellen selbst AGB dar und sind deshalb an den allgemeinen Anforderungen für AGB zu messen. Sie können den Betroffenen unangemessen benachteiligen und für ihn überraschend sein. Dies gilt insbesondere, wenn sie zu einer vollständigen Aufzeichnung aller Telefonate berechtigen würden, ohne dabei die gesetzlichen Grundgedanken der Datensparsamkeit und Erforderlichkeit zu beachten. Davon wird auszugehen sein, wenn es lediglich einen einzigen telefonischen Kommunikationskanal gibt, der dann auch für Anrufe genutzt werden muss, die kein Bankgeschäft zum Gegenstand haben. Eine solche Gestaltung der AGB ginge über die gesetzlichen Grundgedanken und Regelungen des BDSG weit hinaus und würde wohl von Bankkunden in der Regel auch nicht erwartet.

Bei der Bewertung der Zulässigkeit ist auch der Grundsatz der Datenvermeidung und der Datensparsamkeit (§ 3a BDSG) zu beachten. Es wird daher den Banken empfohlen, zwei Hotlines anzubieten. Eine, auf der aufgezeichnet wird, und eine ohne die Möglichkeit der Aufzeichnung, bei der allerdings keine Bankgeschäfte angeboten werden müssen.

Wird nur eine Hotline betrieben oder werden die Gespräche aller Hotlines aufgezeichnet, muss entweder die Möglichkeit bestehen, die Aufzeichnung abzuschalten (bzw. idealerweise für wichtige Erklärungen anzuschalten und damit nicht standardmäßig aufzuzeichnen), oder zumindest das aufgezeichnete Gespräch unmittelbar danach zu überspielen, wenn der Aufzeichnung widersprochen wird.

Um den Kunden vor der Aufzeichnung gesondert in Kenntnis zu setzen, wäre zusätzlich zur Einholung der Einwilligung eine Information über die Aufzeichnung zu Beginn eines jeden Gespräches aus Gründen der Transparenz wünschenswert.

5.3.3.3
Dauer der Speicherung

Als zulässige Speicherdauer von Telefonaufzeichnungen werden sechs Monate ab Aufzeichnung angesehen. Begründen lässt sich dies damit, dass in der Regel über die Inhalte der aufzeichnungsfähigen Anrufe ohnehin eine Bestätigung seitens der Bank erstellt und dem Betroffenen zur Kenntnis gebracht wird. Damit ist eine fortdauernde Speicherung nicht notwendig. Zusätzlich findet in der Regel in diesem Zeitraum ein Rechnungsabschluss statt, so dass auch in diesen Fällen eine Speicherung deutlich über die Bereitstellung des Rechnungsabschlusses hinaus nicht notwendig erscheint.

5.3.3.4
Aktueller Sachstand

In den meisten untersuchten Fällen wurden die vorstehenden Anforderungen nicht vollständig erfüllt. Soweit dies der Fall war, konnte ich die betroffenen Kreditinstitute im Verlauf der Prüfungen davon überzeugen, die Anforderungen vollständig zu erfüllen oder gleichwertige Ersatzlösungen durchzuführen.

5.3.4
Zahlungssysteme mit kontaktloser Bezahlfunktion

Zahlungssysteme wie die Geldkarte girogo, die girocard (EC-Karte) und Kreditkarten enthalten bei Neuausgabe mittlerweile eine Möglichkeit zur kontaktlosen Kommunikation. Aufgrund meiner Anregung hat ein Bankenverband die rechtlich gebotene Datenschutzfolgeabschätzung vervollständigt. Sie wird derzeit von den Aufsichtsbehörden geprüft.

Die Risiken bei dem Betrieb von RFID-Systemen sollen nach einer Empfehlung der Europäischen Kommission besonders untersucht werden. Dazu wurde ein Rahmen für Datenschutzfolgeabschätzungen erstellt, der die Durchführung einer solchen Datenschutzfolgeabschätzung beschreibt (das sog. PIA-Framework).

Die Notwendigkeit, mögliche Risiken vor Beginn der Verarbeitung zu untersuchen und Möglichkeiten zu prüfen, diesen zu begegnen, ist im nationalen Datenschutzrecht in § 4d Abs. 5 BDSG geregelt.

§ 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. *die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens,*

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.

Die Risiken wurden für den grundsätzlichen Betrieb der Zahlungssysteme bereits untersucht. Es sind aber immer noch Einsatzgebiete denkbar, deren Risiken noch nicht betrachtet wurden.

Durch eine Presseveröffentlichung wurde ich auf den Einsatz eines Zahlungssystems aufmerksam, dessen Risiken noch nicht im Rahmen einer Datenschutzfolgeabschätzung vollständig untersucht wurden. Das Zahlungssystem konnte insbesondere Zahlungen ohne Verwendung eines zertifizierten Terminals auslösen. Anstelle eines solchen Terminals wurde ein Smartphone eingesetzt. Dieses besondere Risiko ist nach meiner Auffassung zu untersuchen.

Daher habe ich den zuständigen Bankenverband, der das Zahlungssystem in den Verkehr gebracht hat, veranlasst, die Datenschutzfolgeabschätzung für dieses System zu ergänzen. Der Entwurf einer solchen Ergänzung liegt mittlerweile vor und wird von den Datenschutzaufsichtsbehörden geprüft.

5.3.5
Herausgabe von Adressen der Mitgesellschafter durch Anlagegesellschaften

Die Herausgabe der Namen von Mitgesellschaftern kann vom Fondsverwalter abgelehnt werden, wenn im Einzelfall Hinweise darauf vorliegen, dass die Herausgabe ausschließlich zu Missbrauchszwecken begehrt wird.

Anlagefonds, die in der Form einer GmbH & Co. KG organisiert sind, bieten in der Regel eine Beteiligung am Fonds durch Übernahme von Gesell-

schaftsanteilen an. Dadurch haben sie eine Vielzahl an Gesellschaftern. Diese sind häufig nur an einer Kapitalbeteiligung und der Erwirtschaftung von Renditen interessiert. An der Wahrnehmung von Gesellschafterrechten besteht nur selten ein Interesse, solange in ausreichendem Umfang Renditen fließen und der Wert der Beteiligung nicht bedroht ist. Zur Wahrung des Datenschutzes wird deshalb in den Anlagefonds meistens der Anspruch einzelner Gesellschafter ausgeschlossen, die Namen der anderen Gesellschafter zu erfahren. Diese Beschränkung wurde durch den BGH in zwei Entscheidungen für unwirksam erklärt, woraus sich einige Beschwerden ergeben haben.

Wächst während der Beteiligung am Fonds das Interesse zur Einberufung einer Gesellschafterversammlung, ist dies erschwert, wenn die Namen der anderen Gesellschafter nicht bekannt sind. Der BGH hatte deshalb die Frage zu klären, ob das Interesse an der Geheimhaltung der Gesellschafter hinter dem Interesse an der Wahrnehmung von Gesellschafterrechten zurückzutreten hat. In zwei Entscheidungen vom 5. Februar 2013 (II ZR 134/11, NJW 2013, 2190, und II ZR 136/11, ZIP 2130, 619) hat der BGH entschieden, dass das Recht, die Namen der anderen Gesellschafter zu kennen, nicht entzogen werden kann.

In der Folge wurde ich von einzelnen Gesellschaftern und Kreditinstituten gefragt, ob sie sich gegen ein Verlangen nach Herausgabe der Namen von Mitgesellschaftern wenden können. Läge in der Herausgabe der Namen ein Verstoß gegen den Datenschutz vor, wäre dies grundsätzlich möglich und ich könnte eine Herausgabe untersagen.

Eine Herausgabe der Namen wird von mir jedoch nicht generell als Verstoß gegen datenschutzrechtliche Bestimmungen betrachtet. Vielmehr kann sich ein solcher Anspruch aus dem Gesellschaftsrecht ergeben. Der BGH hat hierzu ausgeführt:

„Ein Anleger, der sich mittelbar über eine Treuhänderin an einer Publikumsgesellschaft beteiligt hat, hat gegen die Gesellschaft und die geschäftsführende Gesellschafterin einen Anspruch darauf, dass ihm die Namen und die Anschriften der (anderen) mittelbar und unmittelbar beteiligten Anleger mitgeteilt werden, wenn er nach den vertraglichen Bestimmungen, insbesondere der Verzahnung des Gesellschafts- und des Treuhandvertrages, im Innenverhältnis der Gesellschafter untereinander und zur Gesellschaft die einem unmittelbaren Gesellschafter entsprechende Rechtsstellung erlangt hat.“

Ob im Einzelfall ein solcher Anspruch besteht, ist von dem jeweiligen Kreditinstitut, Fondsverwalter oder Fondstreuhänder sorgfältig zu überprüfen.

Dabei begrüße ich es, wenn bei jedem einzelnen Herausgabeverlangen zwischen den unbeschränkbaren Rechten des Gesellschafters und den gleichwohl bestehen bleibenden Vorschriften des Datenschutzes und damit den schutzwürdigen Interessen anderer Gesellschafter eine Abwägung getroffen wird. Dies gilt ganz besonders in den Fällen, in denen andere Gesellschafter durch die Wahl der Beteiligungsart ein besonderes Schutzinteresse ausgedrückt haben. Kommt der auf Herausgabe der Adressdaten in Anspruch Genommene dabei zu dem Ergebnis, dass ein Anspruch auf Herausgabe der Adressdaten nicht besteht, ist dies datenschutzrechtlich nicht zu bemängeln.

Zwar haben die Gesellschafterrechte gegenüber den Anonymitätsinteressen der Kommanditisten und Treuhandkommanditisten generell Vorrang. Dennoch hat der BGH in den Urteilen zu erkennen gegeben, dass ein Missbrauch dieses Rechtes und damit ein Verstoß gegen den Datenschutz nicht auszuschließen ist. Hat ein in Anspruch genommener Fondsverwalter daher im Einzelfall Hinweise darauf, dass die Herausgabe der Daten ausschließlich zu Missbrauchszwecken begehrt wird und Gesellschafterrechte beim Herausgabeverlangen keine Rolle spielen, halte ich eine Herausgabeverweigerung auch im Hinblick auf die zitierten Urteile des BGH für gerechtfertigt. Dies gilt insb. dann, wenn die Gesellschafterrechte, die wahrgenommen werden sollen, auch ohne Kenntnis der Adressen anderer Gesellschafter wahrgenommen werden können.

Ein Missbrauchsverdacht kann sich z. B. aus einem bereits erfolgten Missbrauch nach einem früher erfolgreich geltend gemachten Herausgabeverlangen ergeben. Wurden die herausgegebenen Adressen durch einen Gesellschafter oder einen von ihm Bevollmächtigten zu Werbezwecken missbraucht, dürfte ein solcher Verdacht zumindest dann vorliegen, wenn keine individuellen Gründe für das Herausgabeverlangen genannt werden.

5.3.6
Complianceanforderungen einer Ratingagentur

Aus Anlass einer Beschwerde habe ich überprüft, ob die Anforderungen an die Compliance in einer Frankfurter Ratingagentur auch die Anforderungen des Datenschutzes in ausreichendem Umfang berücksichtigen. Soweit dies nicht der Fall war, konnte ich eine Änderung des europaweiten Complianceкonzeptes erreichen.

Ratingagenturen unterliegen der Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009. Gemäß Art. 7 Abs. 3 in Verbindung mit Anhang I Abschnitt C der Verordnung haben

Ratingagenturen sicherzustellen, dass es zu keinen Interessenkonflikten und Insidergeschäften bei Mitarbeitern kommt, die direkt an Ratingtätigkeiten beteiligt sind. Diese Verpflichtung erstreckt sich auch auf Personen, die mit den zu überwachenden Mitarbeitern in enger Beziehung stehen.

Zur Erfüllung der Verordnung wurden im Rahmen des geprüften Compliancekonzeptes alle Mitarbeiter und diesen nahestehenden Personen zur laufenden Offenlegung ihrer Finanzgeschäfte aufgefordert. Dabei wurde nicht nach der jeweiligen Tätigkeit differenziert. Insb. wurde dabei nicht beachtet, ob der jeweilige Mitarbeiter tatsächlich direkt an Ratingtätigkeiten beteiligt war.

Auch wenn ein hohes und gesetzlich legitimiertes Interesse an der Überwachung von Mitarbeitern besteht, hebt dies die Anforderungen des Datenschutzes nicht auf. Deshalb muss ein Compliancekonzept nach der Tätigkeit der Mitarbeiter unterscheiden und den Grad der Überwachung daran ausrichten. Ein Konzept ohne eine derartige Differenzierung halte ich nicht für zulässig.

Davon war auch die Ratingagentur zu überzeugen. Das Compliancekonzept wurde auf meine Intervention geändert, ein abgestuftes System vorgelegt und durch die Ratingagentur europaweit eingeführt.

5.3.7
Verwendung von Kontodaten auf vorgedruckten Überweisungsträgern bei Spendenaufrufen

Spendensammler dürfen die von ihrer Bank übermittelten Kontodaten von Spendern nicht zum Zwecke der Spendenwerbung nutzen.

Durch eine Eingabe wurde ich darauf aufmerksam, dass ein eingetragener Verein Spendenaufrufe an Personen versandt hat, die bereits in der Vergangenheit an diesen Spendensammler gespendet hatten. Diese Spenden wurden dabei von den Betroffenen auf das Konto des Vereins überwiesen, der aus seinen Kontoauszügen die Kontodaten der Spender entnehmen konnte. Um weitere Spenden zu generieren, schrieb der Verein die Betroffenen daraufhin an. Dem Spendenaufruf-Schreiben lag ein Überweisungsträger bei, der neben den Daten des Vereins auch den Namen und die Kontodaten (Kontonummer und Bankleitzahl/IBAN und BIC) des potenziellen Spenders enthielt. In der mir vorliegenden Eingabe wurde nach der Rechtmäßigkeit der Nutzung dieser Daten gefragt.

Zum Zweck der Werbung dürfen ausschließlich Daten verwendet werden, die zulässigerweise erhoben worden sind. Zulässig ist eine Direkterhebung

beim Betroffenen oder die Erhebung aus einer öffentlichen Quelle. Beides trifft auf die Erhebung von Kontodaten, die dem Spendensammler durch seine Bank übermittelt worden sind, nicht zu. Eine Ausnahme der Nutzung von Daten ohne Einwilligung stellt der § 28 Abs. 3 BDSG dar.

§ 28 Abs. 1, 3 und 5 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) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. *für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,*
2. *für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder*
3. *für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind.*

Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

...

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

Dieser erlaubt jedoch ausschließlich die Nutzung von Listendaten, zu denen die Kontodaten nicht zählen. Daher wäre für die Nutzung zu Werbezwecken eine Einwilligung der Betroffenen notwendig. Diese kann auch nicht dadurch konstruiert werden, dass die Betroffenen ihre IBAN und BIC auf dem Überweisungsträger angegeben haben und die Bank diese im Rahmen der Überweisung an den Verein übermittelt hat. Vielmehr sind diese Daten zur Ausführung der Überweisung notwendig und dürfen daher von der Bank auch erhoben werden (§ 28 Abs. 1 BDSG). Eine Einwilligung zur Verwendung dieser Daten zum Zwecke der Werbung liegt in keinem Fall vor.

Nach § 28 Abs. 5 BDSG dürfen Daten von einem Dritten nur für den Zweck verarbeitet oder genutzt werden, zu dessen Erfüllung sie übermittelt werden. In der vorliegenden Fallkonstellation ist dies ganz eindeutig nicht zum Zwecke der Werbung, sondern zur Durchführung des Zahlungsverkehrs.

Da weder eine rechtliche Grundlage noch eine Zustimmung der Betroffenen zur Verwendung zu Werbezwecken vorliegt, ist die hier dargestellte Nutzung der Daten unzulässig.

Ich habe den Verein nach Prüfung des Sachverhaltes aufgefordert, die bisherige Praxis einzustellen.

5.3.8
SCHUFA Holding AG

Das Scoring der SCHUFA gab keinen Anlass zur Kritik.

Hinsichtlich des Inhalts der Datenübersicht für Betroffene und des Verfahrens zum Erhalt einer Datenübersicht hat die Schufa aufgrund meiner Kritik Änderungen vorgenommen.

Die SCHUFA Holding AG, die nach eigenen Angaben zu mehr als 66 Mio. Personen Daten speichert, bildete auch im aktuellen Berichtszeitraum wieder einen wesentlichen Schwerpunkt meiner Prüfungstätigkeit. In keinem anderen Bereich als der Tätigkeit von Handelsauskunfteien gehen bei mir mehr Beschwerden ein.

5.3.8.1
Scoring der SCHUFA

Das Scoring der SCHUFA wurde von mir im Berichtszeitraum wieder besonders intensiv betrachtet. Das Scoring ist seit dem Jahr 2010 in § 28b BDSG gesetzlich geregelt.

§ 28b BDSG

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. *die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,*
2. *im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,*
3. *für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,*
4. *im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.*

Zur Ermittlung von Scorewerten lagen zahlreiche Beschwerden vor. Bei diesen kann ich nur überprüfen, ob der Scorewert entsprechend den gesetzlichen Regelungen ermittelt wurde. Ob der Scorewert inhaltlich richtig ist und den Betroffenen zutreffend beschreibt, kann nicht überprüft werden. Im Regelfall ergab sich bereits aus dem Sachverhalt der Beschwerde kein Verstoß gegen § 28b BDSG. In diesen Fällen wurde den Beschwerdeführern der Vorgang des Scorings sowie die gesetzlichen Vorschriften erläutert.

Soweit sich aus den jeweils ermittelten Beschwerden Zweifel an den Scorewerten, vor allem an der Erheblichkeit der verwendeten Daten für die Berechnung eines schlechten Scorewertes ergaben, wurde die SCHUFA um Offenlegung der Gründe für den ermittelten Scorewert gebeten. In allen Fällen konnte die SCHUFA den Nachweis führen, dass der im Einzelfall ermittelte Scorewert den Anforderungen von § 28b BDSG, insb. den Anforderungen von § 28b Nr. 1 BDSG, entsprach.

Außerdem wurden mit der SCHUFA mehrere gemeinsame Termine durchgeführt, in denen das Grundprinzip und Einzelheiten des Scorings durch die SCHUFA ausführlich erläutert wurden.

Die einzelnen Merkmale, die zur Ermittlung der Scorewerte verwendet werden, wurden von der SCHUFA bereits im Jahr 2010 im Einzelnen mir gegenüber offengelegt. Die SCHUFA verwendet für unterschiedliche Zwecke und Vertragspartner abweichende Scorekarten mit jeweils unterschiedlichen Merkmalen. Die wesentlichsten Scorekarten und die für die jeweilige Berechnung verwendeten Merkmale wurden bereits im Jahr 2010 offengelegt. Im Berichtszeitraum wurde die SCHUFA nun gebeten, die Abweichungen zwischen den unterschiedlichen Scorekarten noch einmal genauer und über die Verwendung unterschiedlicher Merkmale hinaus zu erläutern. Die SCHUFA konnte dabei nachvollziehbar darstellen, welche Abweichungen in den unterschiedlichen Scorekarten bestehen und warum diese bei deren Verwendung zu unterschiedlichen Ergebnissen führen können. Zweifel an der Erfüllung der gesetzlichen Anforderungen des § 28b BDSG ergaben sich daraus nicht.

Im Rahmen der Prüfungen wurde die SCHUFA außerdem aufgefordert, ein besonders umstrittenes Merkmal, die Anzahl der Voranschriften, detailliert zu erläutern. Die SCHUFA konnte hierbei plausibel belegen, dass die Verwendung des Merkmals die gesetzlichen Anforderungen erfüllt. Insbesondere haben sich keine Zweifel an der statistischen Signifikanz des Merkmals ergeben.

Die SCHUFA hat dabei auch die Berechnung der Scorewerte noch einmal näher erläutert. Die Ermittlung der Scorewerte erfolgt durch eine statistische Auswertung der gespeicherten Daten und der Bestimmung von statistischen Beziehungen zwischen den in der Scorecard verwendeten Merkmalen. Dabei spielt insbesondere die Beziehung zum Auftreten von Forderungsausfällen und Vertragsstörungen eine Rolle. Zwar verknüpft die SCHUFA einzelne Merkmale und deren Beziehung zu Forderungsausfällen und Vertragsstörungen anschließend mittels einer Formel unter Gewichtung der Ergebnisse miteinander. Für das Ergebnis entscheidender als die Formel zur Verknüpfung einzelner Merkmale erscheint jedoch die statistische Auswertung der Korrelationen.

Bereits die Gewichtung und Verknüpfung einzelner Merkmale miteinander mittels einer Formel basiert auf statistischen Signifikanzanalysen der gespeicherten Daten. Vor allem aber die Ermittlung der statistischen Zusammenhänge zwischen einzelnen Merkmalen einerseits und Forderungsausfällen sowie Vertragsstörungen andererseits basieren auf den von der SCHUFA gespeicherten Daten.

Bei der Beurteilung ist zu berücksichtigen, dass diese einen wesentlichen Teil des Unternehmenswertes der SCHUFA darstellen. Die SCHUFA hat daher an der Geheimhaltung von statistischen Auswertungen dieser Daten ein

berechtigtes Interesse. Die statistische Auswertung ist außerdem nicht offenkundig. Folglich stellen derartige Auswertungen auch Betriebsgeheimnisse der SCHUFA dar, die im Rahmen einer Selbstauskunft nach § 34 BDSG nicht offengelegt werden müssen.

Diese Sichtweise wurde auch durch den Bundesgerichtshof in seinem Urteil vom 28. Januar 2014 (Az. VI ZR 156/13, BGHZ 200, 38-51 = NJW 2014, 1235-1238) bestätigt.

Teilweise wird gefordert, dass jedenfalls die Gewichtung einzelner Merkmale gegenüber dem jeweiligen Betroffenen offengelegt werden müsse. Wie bereits ausgeführt, kann es sich bereits bei der Gewichtung der Ergebnisse zueinander um Betriebsgeheimnisse handeln. Deren Offenlegung könnte die Transparenz der Scorewertberechnung zwar erhöhen. Der wesentliche Teil der Bestimmung von Scorewerten sind jedoch die statistischen Korrelationen. Ohne Offenlegung der statistischen Korrelationen ist eine Scorewertberechnung auch bei Kenntnis der Gewichtung einzelner Merkmale nicht überprüfbar. Zur Erreichung von Transparenz genügen die Offenlegung der verwendeten Merkmale und deren Gewichtung deshalb nicht.

Nicht zu verkennen ist jedoch, dass Scorewerte nicht selten auf einer im Verhältnis zu den aussagefähigen Daten über eine Person sehr geringen Datenbasis und damit geringen Signifikanz errechnet werden. Betroffene, die einer als riskant ermittelten Risikogruppe zugeordnet werden, müssen nicht zwingend auch ein hohes individuelles Risiko darstellen. Werden zudem von vielen Marktteilnehmern die gleichen Daten zur Errechnung von Scorewerten genutzt, ist die Gefahr gegeben, dass Betroffene bei der Aufnahme von Krediten oder dem Bezug von Produkten mit Kreditrisiko, z. B. beim Mobilfunk, grundlos stark behindert werden. Wichtig ist deshalb, dass Betroffene die Gelegenheit erhalten, die errechneten Scorewerte in einer individuellen Entscheidung des Scoreanwenders (z. B. Kreditinstitute oder Einzelhändler) zu widerlegen. Im Massengeschäft und insbesondere im Onlinehandel dürfte aber nur selten die Gelegenheit bestehen, das pauschal errechnete Risiko individuell zu korrigieren.

Allerdings objektiviert Scoring die daraufhin getroffenen Entscheidungen aufgrund der nachweisbaren statistischen Signifikanz von Merkmalen. Ohne Scoring basiert die Entscheidung auf einem üblicherweise kleinen, zufälligen und subjektiv empfundenen Erfahrungswissen. Richtig angewendet können Entscheidungen unter Verwendung von Scorewerten deshalb treffsicherer sein. In der Beschwerdepraxis haben sich auch keine Hinweise darauf ergeben, dass die verwendeten Verfahren Mängel aufweisen. Zertifizierungen für Scoringverfahren, die vereinzelt gefordert werden, dürften

kaum zur Verbesserung der Scoringergebnisse beitragen. Sie würden aber deren schnelle Anpassung und Verbesserung behindern.

Auch gelegentlich erhobene Forderungen nach einem Nachweis der Kausalität von statistisch signifikanten Korrelationen unterstütze ich nicht. Ein solcher Nachweis wird kaum je zu führen sein, ohne die Zusammenhänge sehr aufwändig zu untersuchen. Ein Erfordernis dieses Nachweises würde deshalb die Anzahl der verwendbaren Merkmale und damit die Qualität des ermittelten Scorings stark reduzieren. Eine solche Verringerung der Scoringqualität ist nicht zielgerecht. Sofern sich eine bei mir erhobene Beschwerde gegen das Scoring gerichtet hat, wurde in aller Regel dessen Qualität bezweifelt und die Verwendung weiterer und im aktuellen Scoring nicht berücksichtigter Merkmale, wie das Einkommen, frühere (und im Datenbestand bereits gelöschte) Kredite oder das Anstellungsverhältnis, gefordert. Diese Merkmale sollten jedoch nicht im Scoring, sondern vielmehr in einer sich anschließenden zweiten Entscheidung durch den Bezieher des Scorewertes berücksichtigt werden.

Außerdem bedarf es eines kausalen Nachweises nicht. Es stehen genügend statistische Methoden zur Fehlerbereinigung zur Verfügung.

Sind bestimmte Merkmale für Kreditrisiken signifikant, dürften diese Merkmale die Betroffenen auch ohne automatisierte Berechnung von Scorewerten bei der Kreditaufnahme behindern. Solche Merkmale dürften nur sehr selten in einer Entscheidung außer Acht bleiben.

Bei den mir vorgelegten Beschwerden wurden Betroffene auch nur in Einzelfällen vom Bezug bestimmter Produkte ausgeschlossen. In diesen Fällen, z. B. fehlende Möglichkeit der Kreditaufnahme während der Privatinsolvenz oder kurz nach Erteilung der Restschuldbefreiung, war dies auch ohne vorheriges Scoring nachvollziehbar.

Sinnvoll erscheint mir allerdings, Betroffene im Falle von Entscheidungen, die ausschließlich oder weit überwiegend auf Scorewerten basieren, über die Entscheidung und den dabei verwendeten Scorewert im Sinne von § 6a Abs. 2 Nr. 2 BDSG zu informieren. Dies sollte sie in die Lage versetzen, die zu ihren Lasten getroffene und weitgehend automatisierte Entscheidung ggf. zu revidieren. Das kann durch die Möglichkeit zur Entkräftung der sie belastenden Umstände oder durch Erläuterung von deren untypischen Ursachen erfolgen.

Dafür ist es allerdings zusätzlich erforderlich, dass dem Unternehmen, welches eine Entscheidung auf der Basis eines Scores getroffen hat, die Datenarten bekannt sind, die sich auf den Score negativ ausgewirkt haben. Sind die negativ wirkenden Datenarten nicht bekannt, der Score also auch

für den Bezieher des Scores und Entscheider eines Unternehmens eine in seinem Zustandekommen vollkommen unbekannte Größe, dürfte ein individuelles Hinwegsetzen über den Scorewert durch einen Sachbearbeiter in der Praxis kaum realistisch sein.

Auch Forderungen nach einem Widerspruchsrecht gegen die Scorewertberechnung sind wenig hilfreich. Ein Unternehmen wird ohne positive Einschätzung der Bonität eines Betroffenen eine Kreditgewährung in der Regel verweigern. Die Scorewertberechnung dient deshalb zu wesentlichen Teilen der positiven Bonitätsbestätigung. Bleibt diese aus, sind die Folgen für den Betroffenen meist schwerwiegender als bei einer nur leicht eingeschränkten Bonitätsbestätigung.

5.3.8.2
Ergänzung der Datenübersicht

Die SCHUFA ist verpflichtet, Betroffenen auf Anforderung umfassend Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen, § 34 BDSG. Die von der SCHUFA erteilte Auskunft wurde nach Form und Inhalt mit dem Regierungspräsidium Darmstadt als früher zuständige Aufsichtsbehörde abgestimmt. Mir ist keine gemäß § 34 BDSG erteilte Auskunft eines anderen Unternehmens bekannt, die umfangreicher wäre.

Durch einen Presseartikel ergaben sich dennoch Zweifel an der Vollständigkeit der erteilten Auskünfte. Eine Prüfung der Auskünfte ergab, dass das Speicherdatum von Merkmalen für Zwecke des Scorings verwendet, in der Datenübersicht aber nicht ausgewiesen wurde.

Ich konnte die SCHUFA davon überzeugen, dass die Datenübersicht entsprechend zu ergänzen ist. Daraufhin wurde das Speicherdatum in die Datenübersicht aufgenommen. Hierzu war die Änderung der zur Auskunftserteilung verwendeten Software erforderlich, so dass die Ergänzung der Auskunft einige Zeit in Anspruch nahm. Bis zur Änderung wurde von der SCHUFA daher das Speicherdatum individuell ergänzt, wenn dies von einem Betroffenen gewünscht wurde.

5.3.8.3
Verfahren zum Erhalt einer Datenübersicht nach § 34 BDSG

Wie in den vergangenen Jahren erhielt ich auch im aktuellen Berichtszeitraum wieder zahlreiche Beschwerden zu der Anforderung der Auskunfteien an die Betroffenen, im Rahmen des Bestellprozesses zum Erhalt einer Datenübersicht nach § 34 BDSG eine Kopie des Personalausweises vorzulegen.

In diesem Zusammenhang wurde durch die Betroffenen wiederholt kritisiert, der Bestellprozess der SCHUFA Holding AG sähe standardisiert eine generelle (und damit unzulässige) Anforderung zur Vorlage einer Personalausweiskopie vor; mithin würde dort eine individuelle Bearbeitung in Form einer differenzierten Einzelfallbetrachtung der Bestellvorgänge grundsätzlich unterbleiben.

Weiterhin wurde durch die Betroffenen kritisiert, die SCHUFA Holding AG würde die Betroffenen über die Möglichkeit der Vornahme von Schwärzungen derjenigen Daten der Personalausweiskopie, die für die Erteilung der Selbstauskunft nicht nötig sind, nicht bzw. nur in unzureichendem Maße aufklären.

Zu beiden Kritikpunkten wurde seitens der Betroffenen jeweils explizit

– auf die „Produktinfo Datenübersicht nach § 34 BDSG“ der Homepage der SCHUFA Holding AG und
– auf die dort veröffentlichten Erläuterungen der SCHUFA Holding AG zu deren „Bestellformular Datenübersicht nach § 34 BDSG“

verwiesen.

Meine – bereits im Jahr 2013 durchgeführte – Analyse der Prozessbeschreibung der SCHUFA Holding AG hinsichtlich der Ausweisanforderung bzw. Auskunftserteilung nach § 34 BDSG hatte ergeben, dass diese eine individuelle Antragsbearbeitung bzw. differenzierte Abläufe hinsichtlich der Anforderung von Ausweisdokumenten vorsehen. Die (beschriebenen) Prozessabläufe gaben mithin keinen Anlass zu einer Kritik meinerseits.

Meine Prüfung der dem Bestellformular vorgeschalteten Webseiten der SCHUFA Holding AG ergab hingegen, dass diese durchaus geeignet waren, bei den Betroffenen den Eindruck einer generellen Anforderung von ungeschwärzten Ausweisdokumenten zu erwecken: Dort war lediglich ausgeführt, das Bestellformular zum Erhalt der Selbstauskunft sei mit einer Kopie des Personalausweises an die SCHUFA Holding AG zu senden.

Fragen der Zulässigkeit der Anforderung von Ausweiskopien sowie der Rahmenbedingungen (u. a. zur Möglichkeit der Vornahme von Schwärzungen auf der Ausweiskopie) habe ich bereits in meinem 41. Tätigkeitsbericht (Ziff. 2.1.2) sowie in meinem 42. Tätigkeitsbericht (Ziff. 4.3.4) erläutert.

Meine Kritik gegenüber der SCHUFA Holding AG hinsichtlich des vorbezeichneten Passus auf der Webseite führte zu einer Löschung der kritisierten Formulierung durch die SCHUFA Holding AG auf deren Homepage. Damit wurden die – an dieser Stelle regelmäßig bei den Betroffenen auftretenden – Unklarheiten und Missverständnisse beseitigt.

Ferner habe ich das „Bestellformular Datenübersicht nach § 34 BDSG“ einschließlich der dort veröffentlichten Erläuterungen der SCHUFA Holding AG, unter anderem hinsichtlich der dort aufgeführten Schwärzungsmöglichkeiten der Ausweiskopie, einer weiteren Prüfung unterzogen. Hierbei stellte sich heraus, dass diese ebenfalls geeignet waren, bei den Betroffenen Unklarheiten/Missverständnisse zu den Fragen aufzuwerfen,

– ob die Übersendung einer Ausweiskopie zwingende Voraussetzung zum Erhalt einer Selbstauskunft ist und
– welche Daten konkret geschwärzt werden können bzw. ob etwa das Passfoto von der Möglichkeit der Schwärzung ausgeschlossen ist.

Von dem Ergebnis meiner Prüfung setzte ich die SCHUFA Holding AG in Kenntnis. Im Rahmen der hierzu geführten Korrespondenz wurden auch an dieser Stelle klarstellende Änderungen der Erläuterungen hinsichtlich der Anforderung einer Ausweiskopie sowie den Schwärzungsmöglichkeiten auf der Ausweiskopie im Rahmen des „Bestellformulars Datenübersicht nach § 34 BDSG“ der SCHUFA Holding AG erreicht.

Letztlich bleibt festzuhalten, dass eine generelle Anforderung hinsichtlich der Vorlage einer Personalausweiskopie durch eine Auskunftei grundsätzlich unzulässig ist.

Sofern jedoch ein Betroffener im Rahmen des Auskunftsersuchens nach § 34 BDSG zur Vermeidung etwaiger Rückfragen durch die Auskunftei dieser eine Ausweiskopie unmittelbar überlässt, wird dies durch mich nicht bemängelt.

5.3.8.4
Identifikation von Betroffenen durch die Kundennummer

Einige Betroffene hatten Schwierigkeiten geschildert, von der SCHUFA eine Datenübersicht nach § 34 BDSG unter Angabe einer SCHUFA-Kundennummer zu erhalten. Die Betroffenen hatten bereits Datenübersichten erhalten, in denen eine von der SCHUFA vergebene Kundennummer angegeben war. Trotz Angabe dieser Kundennummer wurden sie von der SCHUFA zur Einsendung von Ausweiskopien aufgefordert. In allen Fällen hatte sich die Adresse nicht geändert.

Die SCHUFA ist gehalten, vor dem Versand einer Datenübersicht die Anschrift zu überprüfen. Ohne eine solche Überprüfung wäre es möglich, den Versand missbräuchlich an eine vermeintlich neue Anschrift anzufordern. Wurde bereits eine Kundennummer vergeben, wurde auch die Anschrift bereits überprüft.

Ich konnte die SCHUFA daher davon überzeugen, dass durch die bereits erfolgte Prüfung der Anschrift und der eindeutigen Zuordnung einer Kundennummer zu einem Betroffenen keine Verwechslungsgefahr besteht. Auf einen erneuten Nachweis der Adresse kann daher verzichtet werden. Der Versand einer Datenübersicht erfolgt jedoch nur an die bereits geprüfte Adresse.

5.3.8.5 SCHUFA FraudPool

Ich habe mich auf Veranlassung der SCHUFA mehrfach mit dem von der SCHUFA schon länger geplanten SCHUFA FraudPool befasst. Bei dem SCHUFA FraudPool handelt es sich um die Ergänzung der bisherigen Produkte der SCHUFA zur Betrugsprävention. In die neue Datenbank sollen vollendete oder versuchte Vermögensdelikte zum Nachteil vor allem von Kreditinstituten eingemeldet werden, um weitere Tathandlungen zu erschweren.

Die SCHUFA hat mir die Konzepte und Planungen des geplanten SCHUFA FraudPools mehrfach vorgestellt und um deren rechtliche Beurteilung gebeten.

Die grundsätzliche Führung einer solchen Datenbank halte ich gem. §§ 28, 29 BDSG für zulässig. Deren Betrieb unterliegt aber engen Voraussetzungen. Zusätzlich ist das Bankgeheimnis zu beachten.

Die Übermittlung von Daten an den SCHUFA FraudPool ist grundsätzlich zulässig gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die übermittelnden Institute haben ein auch in § 25h Abs. 3 KWG normiertes Interesse an der Beteiligung am SCHUFA FraudPool. Sie erhalten bei Beteiligung und Einmeldung von Daten auch selbst Hinweise aus dem SCHUFA FraudPool, die ihnen zur Verringerung ihres eigenen Betrugsrisikos dienen.

§ 25h Abs. 3 KWG

(3) Jeder Sachverhalt, der nach Absatz 2 Satz 1 als zweifelhaft oder ungewöhnlich anzusehen ist, ist vom Institut zu untersuchen, um das Risiko der jeweiligen Geschäftsbeziehungen oder Transaktionen überwachen, einschätzen und gegebenenfalls das Vorliegen eines nach § 11 Absatz 1 des Geldwäschegesetzes meldepflichtigen Sachverhalts oder die Erstattung einer Strafanzeige gemäß § 158 der Strafprozessordnung prüfen zu können. Über diese Sachverhalte hat das Institut angemessene Informationen nach Maßgabe des § 8 des Geldwäschegesetzes aufzuzeichnen und aufzubewahren, die für die Darlegung gegenüber der Bundesanstalt erforderlich sind, dass diese Sachverhalte nicht darauf schließen lassen, dass eine Tat nach § 261 des Strafgesetzbuchs oder eine Terrorismusfinanzierung begangen oder versucht wurde oder wird. Absatz 2 Satz 2 gilt entsprechend. Institute dürfen im

Einzelfall einander Informationen im Rahmen der Erfüllung ihrer Untersuchungspflicht nach Satz 1 übermitteln, wenn es sich um einen in Bezug auf Geldwäsche, Terrorismusfinanzierung oder einer sonstigen Straftat auffälligen oder ungewöhnlichen Sachverhalt handelt und tatsächliche Anhaltspunkte dafür vorliegen, dass der Empfänger der Informationen diese für die Beurteilung der Frage benötigt, ob der Sachverhalt gemäß § 11 des Geldwäschegesetzes anzuzeigen oder eine Strafanzeige gemäß § 158 der Strafprozessordnung zu erstatten ist. Der Empfänger darf die Informationen ausschließlich zum Zweck der Verhinderung der Geldwäsche, der Terrorismusfinanzierung oder sonstiger strafbarer Handlungen und nur unter den durch das übermittelnde Institut vorgegebenen Bedingungen verwenden.

Sind die Voraussetzungen für die Übermittlung von Daten eines Institutes an den SCHUFA FraudPool erfüllt, dürfen diese dort gem. § 29 Abs. 1 Ziff. 1 BDSG gespeichert und genutzt werden.

Allerdings besteht nur dann, wenn die übermittelten Sachverhalte in ähnlich eindeutiger Weise wie in § 28a Abs. 1 BDSG gesichert festgestellt sind, kein Grund zur Annahme, dass das schutzwürdige Interesse des Betroffenen überwiegt. Dies schließt die Übermittlung bloßer Verdachtsmomente aus und bedingt daher, dass die übermittelten Sachverhalte inkl. der Nachweismöglichkeiten katalogartig aufgeführt sind. Dies ist bei nachweislich gefälschten Ausweispapieren oder bei gefälschten Postident- oder anderen Urkunden, deren Fälschung oder Verfälschung durch den vermeintlichen Aussteller bestätigt wurde, der Fall. Die Meldung von nicht im Einzelnen definiertem betrügerischem Verhalten ist wegen des reinen Verdachtscharakters nicht zulässig.

Sowohl nach Art. 8 Abs. 5 der EG-Datenschutzrichtlinie als auch nach §§ 35 Abs. 2 Ziff. 2, 42a Satz 1 Nr. 3 BDSG sind personenbezogene Daten betreffend strafbare Handlungen besonders geschützt. Diese unterliegen zwar nicht den besonderen Regelungen von §§ 28 Abs. 6 bis 9 und 29 Abs. 5 BDSG. Die Sensibilität dieser Daten ist jedoch im Rahmen der Interessenabwägung der §§ 28 Abs. 1 Satz 1 Nr. 2 und 29 Abs. 1 und 2 BDSG zu berücksichtigen.

Mangels spezialgesetzlicher Regelung ist bei der Übermittlung und Speicherung das Bankgeheimnis zu beachten. Dieses kann durch eine Einwilligung zur Übermittlung der Daten zu diesem Zweck durchbrochen werden. Die aktuell verwendete SCHUFA-Klausel erfüllt diese Voraussetzung.

Eine Auskunft aus dem SCHUFA FraudPool erfordert das Vorliegen eines berechtigten Interesses im Sinne von § 29 Abs. 2 BDSG. Dieses ist auch bei Einholung einer Bonitätsauskunft erforderlich. Wird daher eine Bonitätsauskunft eingeholt und liegt für diese ein berechtigtes Interesse im Sinne

von § 29 Abs. 2 BDSG vor, besteht in der Regel auch ein berechtigtes Interesse für eine Auskunft aus dem SCHUFA FraudPool.

Bei dem Betrieb des SCHUFA FraudPools sind außerdem alle sonstigen Regelungen des BDSG zu beachten. Insbesondere haben Betroffene ein Recht auf Auskunft gem. § 34 BDSG und auf Berichtigung, Löschung und Sperrung gem. § 35 BDSG.

Anfragen an den SCHUFA FraudPool erfolgen bundesweit durch Vertragspartner der SCHUFA. Auch andere Handelsauskunfteien können Produkte mit ähnlicher Zielrichtung anbieten. Die Datenschutzaufsichtsbehörden der Länder und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit haben sich daher auf meinen Vorschlag mit allgemeinen Kriterien für Betrugspräventionssysteme befasst und sich auf einen umfassenden Kriterienkatalog verständigt. Den Betrieb und die weitere Entwicklung des SCHUFA FraudPools werde ich unter Berücksichtigung dieses Kriterienkataloges weiter kritisch überwachen.

5.3.8.6
Vermieterauskunft

Trotz Stellung einer Kaution besteht für den Vermieter ein erhebliches finanzielles Risiko bei Eingehung und Durchführung eines Mietvertrages. Die überlassene Wohnung hat einen erheblichen Wert und die laufenden Mietzahlungen sind nur für wenige Monate durch die Kaution abgesichert. Vermieter haben daher ein berechtigtes Interesse an der Einholung einer Bonitätsauskunft bei einer Auskunftei.

Andererseits handelt es sich bei der Anmietung einer Wohnung für den potenziellen Mieter um die Befriedigung eines Grundbedürfnisses. Ohne die Möglichkeit zur Anmietung einer Wohnung droht der Ausschluss aus der Gesellschaft. Daher ist die Einholung einer Bonitätsauskunft durch den Vermieter nur eingeschränkt zulässig.

In diversen Gesprächen mit der SCHUFA wurde eine Lösung gefunden, in der die Interessen beider Parteien ausreichend berücksichtigt sind. Insbesondere werden bei Auskünften an Vermieter nur Forderungen berücksichtigt, bei denen die aufgetretenen Zahlungsstörungen nur eine relativ kurze Zeit zurückliegen. Hierdurch können Probleme aufgrund von Negativeintragungen in einem überschaubaren Zeitraum überwunden werden.

Außerdem werden von Vermietern gemeldete Forderungen nur bei Vorliegen zusätzlicher Voraussetzungen in den Datenbestand der SCHUFA aufgenommen. Dies trägt den häufig schwer zu erfassenden Streitigkeiten nach Beendigung eines Mietverhältnisses Rechnung.

5.3.9
Auskunft ohne Nachweis der Richtigkeit nach Widerspruch unzulässig

Auskunfteien dürfen bestrittene Daten, deren Richtigkeit sie nicht nachweisen können, für Auskunftszwecke nicht verwenden.

Bereits im Jahr 2012 erhielt ich eine Beschwerde über eine hessische Auskunftei. Der Auskunftei wurde vorgeworfen, nach dem Bestreiten der Richtigkeit von Daten durch eine Betroffene eine unzulässige Auskunft zu erteilen.

Der Grund für die Unzulässigkeit der Auskunft ist in § 35 Abs. 4a BDSG enthalten.

> *§ 35 Abs. 4 und 4a BDSG*
>
> *(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.*

Nachdem sich die Betroffene gegen die Richtigkeit von Daten gewandt hatte, die durch die Auskunftei gespeichert waren, wurden dort die Daten gesperrt. Anfragen wurden durch die Auskunftei jedoch stets so beantwortet, dass durch den Anfrager auf die Speicherung von Daten geschlossen wurde. Die Auskunftei teilte sinngemäß mit, dass derzeit eine Auskunft nicht möglich sei.

Derartige Auskünfte belasten Betroffene unzumutbar. Anfrager schließen aus derartigen Auskünften in der Regel auf Negativtatsachen. Entsprechend konnte die Betroffene keine Geschäfte mehr tätigen.

Auch auf meinen Hinweis, dass eine derartige Praxis unzulässig sei, wurde die Auskunft nicht geändert. Zusätzlich stellte sich im Verlauf der Prüfungen heraus, dass die Auskunftei die schriftliche Benachrichtigung der Betroffenen gem. § 33 BDSG nicht nachweisen konnte.

Aufgrund dessen habe ich gegen die Auskunftei eine Anordnung gem. § 38 Abs. 5 Satz 1 BDSG erlassen. Die Anordnung verpflichtet die Auskunftei, im Falle der Sperrung von Daten eine neutrale Auskunft zu erteilen, die nicht auf die Speicherung von Daten hindeutet. Dies kann die wahrheitswidrige Auskunft erfordern, dass keine Daten gespeichert sind. Darüber hinaus habe ich angeordnet, dass Benachrichtigungen gem. § 33 BDSG für die Dauer von sechs Jahren aufzubewahren sind.

Die Auskunftei hat sich gegen die erlassene Anordnung mit einer Klage sowie einem Eilantrag vor dem Verwaltungsgericht Darmstadt gewendet. Das

Verwaltungsgericht Darmstadt hat den Eilantrag mit Beschluss vom 21. Mai 2013 (Az: 5 L 304/13.DA) abgelehnt. Der Verwaltungsgerichtshof Kassel hat die Beschwerde der Auskunftei gegen den Beschluss des Verwaltungsgerichts Darmstadt durch Beschluss vom 2. Januar 2014 (Az: 10 B 1397/13) zurückgewiesen. Daraufhin hat die Auskunftei die Klage im Hauptsacheverfahren zurückgenommen. Die Anordnung ist damit bestandskräftig geworden.

Durch dieses Verfahren wurden die Rechtslage bei Sperrung von Daten und die in diesem Fall zu erteilende Auskunft endgültig geklärt. Auskunfteien dürfen bestrittene Daten, deren Richtigkeit sie nicht nachweisen können, für Auskunftszwecke nicht verwenden. Solche Daten sind im Rahmen der Auskunft vielmehr so zu behandeln, als wären sie nicht gespeichert. Auch die Auskunft ist so zu erteilen, als wären die Daten nicht gespeichert. In vielen Fällen dürfte dies bedeuten, dass mit der Auskunft die Aussage verbunden ist, zu bestimmten Datenarten keine Daten gespeichert zu haben.

Diese Aussage mag bewusst falsch sein. Anders ist jedoch der gesetzgeberische Anspruch aus § 34 Abs. 4a BDSG nicht zu erfüllen.

5.3.10
Speicherung und Verarbeitung von Anschriftendaten durch die SCHUFA Holding AG

Auskunfteien speichern die Adressen und teilweise auch die ehemaligen Adressen der ihnen bekannten Personen. Diese Anschriftendaten sind für die Tätigkeit der Auskunfteien nicht nur nützlich, sondern auch grundlegend erforderlich. Dennoch ist die Speicherung von Anschriftendaten nicht unbegrenzt zulässig.

Immer wieder erreichen mich Beschwerden über die Speicherung und Verwendung von Anschriftendaten durch die SCHUFA Holding AG. Häufig richten sich die Beschwerden gegen die Dauer der Speicherung von Voranschriften, also von ehemaligen Anschriften der Betroffenen, und gegen die Aufforderung der SCHUFA Holding AG, Voranschriften zu nennen, damit eine Selbstauskunft erteilt werden kann. Aufgrund dieser Beschwerden habe ich die Erhebung, Speicherung und Verarbeitung von Anschriftendaten durch die SCHUFA Holding AG eingehend untersucht und die Grenzen der Verarbeitung von Adressdaten durch Auskunfteien aufgezeigt.

Zu jeder ihr bekannten Person hat die SCHUFA Holding AG mindestens eine Anschrift gespeichert. Diese Anschriftendaten verwendet die Auskunftei zu verschiedenen Zwecken. So wird die Anschrift vor allem zur Identifizierung der angefragten Personen genutzt. Neben dem Namen und dem Geburts-

datum ist die Anschrift die entscheidende Angabe, um Personen eindeutig identifizieren bzw. individualisieren zu können. Da die Anschrift durch Umzüge aber häufiger als andere Merkmale wechseln kann, werden von der SCHUFA Holding AG auch ehemalige Anschriften gespeichert. So kann eine Person auch dann noch eindeutig zugeordnet werden, wenn ihre neue Adresse noch nicht bei allen ihren Vertragspartnern bekannt ist. Die SCHUFA Holding AG fragt sogar gezielt nach ehemaligen Anschriften, wenn eine Person, die eine Selbstauskunft nach § 34 Abs. 4 BDSG verlangt, nicht eindeutig identifiziert werden kann. Dies ist beispielsweise der Fall, wenn es Abweichungen zwischen der bei der SCHUFA Holding AG gespeicherten und der vom Betroffenen angegebenen Adresse gibt.

§ 34 Abs. 4 BDSG

Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. *die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,*
2. *die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,*
3. *die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie*
4. *das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.*

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. *die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder*
2. *bei einer anderen Stelle gespeicherte Daten nutzt.*

Anschriftendaten werden von der SCHUFA Holding AG aber auch für weitere Zwecke verwendet. So findet die Anzahl der zu einer Person gespeicherten Anschriften beispielsweise Eingang in deren Scoring. Zudem bietet die SCHUFA Holding AG bestimmte adressbezogene Produkte an, bei denen die Er- und Übermittlung der Anschriften von Personen im Vordergrund stehen.

Im Rahmen der Konsultationen zu diesem Thema hat die SCHUFA Holding AG dargelegt, welche Anschriftendaten von ihr gespeichert werden. Dabei gilt der Grundsatz, dass jeder Person nur eine aktuelle Adresse zugewiesen ist. Diese wird ersetzt und damit automatisch zur Voranschrift, wenn der Auskunftei eine neuere Anschrift der betroffenen Person bekannt wird. Dieses Verfahren führt jedoch teilweise zu dem Problem, dass noch aktuelle

Anschriften von Betroffenen mit anderen Anschriften wie z. B. mit deren Geschäftsadressen „überschrieben“ werden. Dies kann beispielsweise dann passieren, wenn die Betroffenen Verträge unter Angabe dieser zweiten Anschrift abschließen und der jeweilige Vertragspartner diese an die SCHUFA Holding AG meldet.

Die SCHUFA Holding AG hat in Besprechungen mit mir im Detail nachgewiesen, dass Anschriftendaten für die erfolgreiche Identifikation von Betroffenen entscheidend sind und dass auch ehemalige Anschriften häufig noch der Zuordnung von Daten dienen. Ebenfalls konnte gezeigt werden, dass sich die Anzahl der gespeicherten Voranschriften statistisch auf die Bonität einer Person auswirkt.

Allerdings wurde durch meine Behörde gegenüber der SCHUFA Holding AG auch klargestellt, dass die Speicherung von Anschriftendaten, und insbesondere die Speicherung von Voranschriften, nicht unbegrenzt zulässig ist. So sind Auskunfteien gem. § 35 Abs. 2 Nr. 4 BDSG gesetzlich dazu verpflichtet, in bestimmten Zeitabständen zu überprüfen, ob die gespeicherten Daten weiterhin gespeichert werden dürfen oder ob sie zu löschen sind.

§ 35 Abs. 2 Nr. 4 BDSG

Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

...

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 längerwährende Speicherung nicht erforderlich ist.

...

Somit dürfen auch Voranschriften nur so lange bei Auskunfteien gespeichert werden, bis bei der gesetzlich vorgeschriebenen Prüfung festgestellt wurde, dass ihre weitere Speicherung nicht mehr erforderlich ist. Inwieweit die Speicherung von Anschriftendaten aus Sicht der Auskunftei erforderlich ist, richtet sich auch nach dem mit der Verarbeitung der Anschriftendaten jeweils verfolgten Zweck.

Im Rahmen des noch andauernden Prozesses werde ich die Speicherung, Verarbeitung und fristgerechte Löschung von Anschriftendaten durch die SCHUFA Holding AG und andere Auskunfteien weiter beobachten und überprüfen. Zudem begleite ich, unter anderem in diesem Punkt, die Weiterentwicklung der Verfahren und Prozesse bei der SCHUFA Holding AG.

5.3.11
Auskunftserteilung gemäß § 34 BDSG durch Inkassounternehmen

Bei Prüfungen habe ich festgestellt, dass einige Inkassounternehmen unvollständige Auskünfte erteilt haben. Die Auskünfte wurden mit meiner Beratung neu gestaltet und erweitert.

Im Berichtszeitraum erreichten mich Beschwerden über unterlassene Auskunftserteilungen durch Inkassounternehmen. Diese nahm ich zum Anlass, die Auskunftspraxis der verantwortlichen Inkassounternehmen einer Prüfung zu unterziehen. Hierbei habe ich mir unter anderem – nach erfolgter Auskunftserteilung durch die Inkassounternehmen – die erteilten Selbstauskünfte zu den jeweiligen Beschwerdeführern vorlegen lassen. Eine Prüfung dieser Selbstauskünfte ergab, dass sie den gesetzlichen Anforderungen nicht genügten. Sie waren unvollständig, weil sie einige der Daten, die für das Forderungsmanagement regelmäßig in branchenüblicher Inkassosoftware gespeichert werden, nicht auswiesen.

Diesen Sachverhalt kritisierte ich gegenüber den verantwortlichen Unternehmen und beriet diese im Rahmen einer Neugestaltung und Erweiterung der Selbstauskünfte über erforderliche Inhalte. Damit konnte im Ergebnis eine deutliche Verbesserung der Auskunftspraxis der verantwortlichen Inkassounternehmen erreicht werden.

Der Umfang der Auskunftsverpflichtung (auch) der Inkassounternehmen ergibt sich aus § 34 Abs. 1 Nr. 1 bis 3 BDSG.

> *§ 34 Abs. 1 Nr. 1 bis 3 BDSG*
>
> *(1) 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.*

Folglich haben Inkassounternehmen dem Betroffenen auch über gespeicherte Anschriften- und Kommunikationsdaten (Telefonnummer, E-Mail-Adresse etc.), Forderungsdaten (Haupt- und Nebenforderungen, Rechnungs- bzw. Titeldaten) und Daten des Gläubigers Auskunft zu erteilen.

5.3.12
Neue Rubrik „Häufig gestellte Fragen“ auf meinem Internetauftritt

Zu den Sachgebieten Auskunfteien, Scoring der Auskunfteien, Banken und Inkasso erhalte ich besonders viele Eingaben. Viele Fragen werden so häu-

fig gestellt, dass ich diese nun in einer neuen Rubrik „Häufig gestellte Fragen“ auf meinem Internetauftritt beantworte.

Die am häufigsten gestellten Fragen betreffen vor allem die Rechte von Betroffenen gegenüber den Auskunfteien und das von diesen durchgeführte Scoring. Zum Scoring habe ich deshalb allgemeine Erläuterungen hinzugefügt, um die Grundlagen des Scorings für Betroffene leichter verständlich zu machen.

Die Inhalte behandeln aber nicht zuletzt auch die Möglichkeiten und Anforderungen zum Erhalt einer Übersicht der von Auskunfteien gespeicherten Daten und Hinweise zum Vorgehen, sollten die Daten einmal fehlerhaft gespeichert worden sein.

Die Hinweise in der neuen Rubrik sollen den Betroffenen einfach und schnell Antworten geben, ohne eine individuelle Eingabe stellen zu müssen. Individuelle Eingaben und telefonische Anfragen sind aber natürlich auch weiterhin jederzeit möglich.

5.4
Verkehr und Energieversorgung

5.4.1
Personenortung für die Fraport App durch die Fraport AG

Die Fraport AG bietet als eine Hilfe für Flugreisende und andere Besucher des Flughafens die Fraport App an. Mit dieser App soll es auch ermöglicht werden, den eigenen Standort anzeigen zu lassen. Die Feststellung des Standorts funktioniert jedoch mit den Möglichkeiten eines Smartphones nur unzureichend. Deshalb wollte die Fraport AG ein am Markt verfügbares System zur Lokalisierung von Geräten einsetzen, bei dem ich Bedenken hatte. Auf Grund meiner Intervention wurde das System so geändert, dass keine Vorbehalte mehr bestehen.

5.4.1.1
Hintergrund

Anfang des Jahres konfrontierte mich die Fraport AG mit dem Anliegen, die Lokalisierung von Smartphones auf dem Flughafengelände zu ermöglichen. Beabsichtigt war, derartige mobile Geräte durch auf dem Gelände verteilte WLAN-Hotspots mit MAC- und IP-Adressen zu erfassen, sofern ihre WLAN-Schnittstelle aktiv war. Mit den erfassten Daten sollten einerseits die Nutzer

der FraApp ihren Standort bestimmen können. Andererseits **sollte zukünftig auf der Basis der gesammelten Daten nach einer Pseudonymisierung das Nutzerverhalten** analysiert werden können. Als Beispiele für die Analysen wurden genannt die Ermittlung der Flächenaus- bzw. -belastung, die Koordinierung der Warteschlangen beim Einchecken und die Messung der Menschenströme bei der Standortverteilung der Verkaufsgeschäfte.

Datenschutzrechtlich zu betrachten waren drei Szenarien:

– Der Nutzer hat die FraApp auf seinem Gerät installiert und somit in seine Ortung auf dem Flughafengelände bei der Installation eingewilligt (Android-basierte Smartphones) oder die Ortungsdienste aktiviert (iOS). Datenschutzrechtlich bestehen keine Bedenken. Bei datenschutzrechtlich korrekt ausgestalteten Apps ist die beabsichtigte Erfassung der Standortdaten erlaubt.
– Der Nutzer hat sich mit seinem mobilen Gerät an einem WLAN-Access Point angemeldet und eine dynamische IP-Adresse zugeteilt bekommen. Die Erfassung stellt kein datenschutzrechtliches Problem dar.

  Netzwerkbetreiber können eine unmittelbare Identifikation anhand der IP-Adresse grundsätzlich nur bei statischen IP-Adressen vornehmen. WLAN-Hotspots werden aber mit Vergabe von dynamischen IP-Adressen betrieben. Eine Identifikation ist nur möglich, wenn die Nutzer während einer Sitzung selbst personenbezogene oder personenbeziehbare Daten hinterlassen. Dies ist nach den vorliegenden Dokumenten nicht der Fall. Deshalb sind dynamische IP-Adressen in diesem Szenario keine personenbeziehbaren Daten.
– Weder die Installation der FraApp noch die Registrierung am WLAN-Access-Point fand statt. Dann wird beim eingeschalteten WLAN die MAC-Adresse erfasst. Bei diesem Szenario komme ich zu dem Schluss, dass die MAC-Adressen als personenbezogene Daten anzusehen sind und den Regelungen des Hessischen Datenschutzgesetzes/Bundesdatenschutzgesetzes unterliegen. Durch die Zuziehung von Zusatzinformationen ist es grundsätzlich möglich, eine Identifizierung des Gerätebesitzers durchzuführen. Bei der Internetnutzung entstehen viele Situationen, in denen MAC-Adressen mit identifizierenden Daten verknüpfbar sind, insbesondere bei werbefinanzierten Smartphone Apps oder bei der Anmeldung an Web-Portalen. Somit sind die MAC-Adressen als personenbeziehbare Daten einzustufen.

5.4.1.2 Problem

Im ersten Entwurf des mit der Umsetzung beauftragten Softwareunternehmens sollten die personenbeziehbaren MAC-Adressen einen Tag zusammen mit den Standortdaten, die über erreichbare Access-Points errechnet werden, im Klartext gespeichert werden. Danach sollte die MAC-Adresse in ein Pseudonym umgewandelt werden und für weitere Analysen zur Verfügung stehen. In diesem Fall wären auch Standortdaten von Unbeteiligten (Szenario 3) gespeichert worden.

5.4.1.3 Lösung

Deshalb wurde von mir der Fraport AG ein Konzept vorgeschlagen, mit dem das System nach wie vor noch seine Funktionen erfüllen kann, jedoch die Personenbeziehbarkeit entfällt. Die Personenbeziehbarkeit soll durch die Anwendung eines Algorithmus umgangen werden. Zuerst wird die MAC-Adresse gekürzt, dann ein SALT-Wert angehängt, darauf eine Hashfunktion angewendet und das Ergebnis wieder so gekürzt, dass es wie eine reguläre MAC-Adresse aufgebaut ist. Das Ergebnis ist ein Identifikator.

Der SALT-Wert wird in bestimmten Intervallen, mindestens täglich, neu generiert. Dadurch wird gewährleistet, dass die aus den MAC-Adressen gebildeten Identifikatoren nach Ablauf des Intervalls unterschiedlich sind. Eine Wiedererkennung über den Wechsel ist nahezu unmöglich. Der Identifikator soll gebildet werden, bevor eine Verarbeitung zur Standortbestimmung erfolgt und der SALT-Wert muss eine Zufallszahl sein, die nicht persistent, d. h. nur im Hauptspeicher, gespeichert wird.

Die serverbasierte Ortung wurde daraufhin von der Fraport AG wie folgt umgesetzt:

Die MAC-Adressen werden von den Access-Points erfasst und über die sogenannte Mobility Solution Engine (MSE) an einen Server übertragen, wo sie durch „Salzen“, „Hashen“ und „Kürzen“ zu einem anonymen Identifikator transformiert werden. Dabei werden die MAC-Adressen nur im Arbeitsspeicher zum Bilden des Identifikators vorgehalten, danach werden sie sofort gelöscht. Der SALT-Wert erfüllt die o. g. Anforderungen. Der Identifikator und die Access-Point-Daten werden an den Lokalisierungsserver übertragen, der den Standort errechnet. Die MAC-Adresse befindet sich nur kurzzeitig im Arbeitsspeicher, so dass sie für keinen anderen Anwendungsfall genutzt werden kann.

Smartphones können nun per FraApp mit ihrer MAC-Adresse am Lokalisierungsserver ihre Position anfragen. Dazu wird die MAC-Adresse des Smartphones von dem vorgeschalteten Server ebenfalls in den Identifikator umgewandelt, dieser dann an den Lokalisierungsserver übertragen und anschließend die MAC-Adresse gelöscht.

Zum Lokalisierungsserver gehört eine Datenbank mit den Datensätzen „letzter erfasster Standort“ und „Identifikator“. Findet der Lokalisierungsserver einen Datensatz mit dem Identifikator des anfragenden Smartphones, kann er dem Smartphone den Standort zusenden, so dass die App dem Nutzer diesen visualisieren kann. Die Standortdaten werden vom Lokalisierungsserver zum Analyseserver übertragen, damit entsprechende Untersuchungen möglich sind.

Mit den dargestellten Anpassungen habe ich keine Vorbehalte mehr gegen die implementierte Ortungsfunktion der Fraport App.

5.4.2
Datenverarbeitung im Kraftfahrzeug

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der von ihr eingesetzte Arbeitskreis der für den Straßenverkehr zuständigen Referenten haben sich im vergangenen Jahr intensiv mit dem Thema „Datenverarbeitung im Kraftfahrzeug“ auseinandergesetzt.

Die digitale Vernetzung unserer Gesellschaft erfasst unaufhaltsam auch die Kraftfahrzeuge. Bis zu 80 Steuergeräte im modernen Auto verarbeiten die durch das Verhalten des Fahrers verursachten Daten. Die neueren Fahrzeuge senden die auf diese Weise anfallenden Daten auch an die Automobilhersteller. Die dabei verarbeiteten Daten sind zum Teil unmittelbar personenbezogen, zum Teil personenbeziehbar. Aus diesem Grunde haben die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz vom 8./9. Oktober 2014 die unter Ziffer 7.9 abgedruckte Entschließung gefasst.

Auf diese Entschließung hin hat der Verband der Automobilindustrie „Datenschutzprinzipien für vernetzte Fahrzeuge“ entwickelt (s. dazu https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutzprinzipien-fuer-vernetzte-fahrzeuge.html).

Die Datenschutzbeauftragten des Bundes und der Länder sind gegenwärtig ihrerseits mit den von dem Verband veröffentlichten Prinzipien befasst. Nach vorläufiger Bewertung werden die Prinzipien als ein guter Anfang bezeichnet, aber zum Teil auch für zu pauschal gehalten.

Ein Treffen der Datenschutzaufsichtsbehörden mit Vertretern des Verbandes ist anberaumt.

5.5
Handel, Handwerk, Selbstständige und Gewerbetreibende

5.5.1
Datenschutz in Anwaltskanzleien

Das BDSG findet auf Rechtsanwältinnen und Rechtsanwälte als jeweils datenverarbeitende, nicht-öffentliche Stellen Anwendung. Sie sind mir gegenüber gemäß § 38 Abs. 3 BDSG grundsätzlich zur Auskunft verpflichtet. Aufgrund der anwaltlichen Verschwiegenheitspflicht reicht mein Auskunftsrecht im Einzelfall jedenfalls so weit, dass mir eine Einschätzung möglich ist, ob das Mandatsgeheimnis greift oder nicht.

5.5.1.1
Anwendbarkeit des BDSG

Im Rahmen mehrerer Eingaben ging es u. a. um das grundsätzliche Verständnis von Rechtsanwältinnen und Rechtsanwälten für die Rolle als datenverarbeitende Stelle und die Anwendbarkeit des BDSG.

Rechtsanwältinnen und Rechtsanwälte sind nicht-öffentliche Stellen im Sinne von § 2 Abs. 4 S. 1 BDSG. Die Bestimmungen des BDSG gelten für sie, soweit sie gemäß § 1 Abs. 2 Nr. 3 BDSG Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben.

§ 2 Abs. 4 S. 1 BDSG

Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen.

§ 1 Abs. 2 Nr. 3 BDSG

Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

…

3. *nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.*

In der Korrespondenz mit einzelnen Rechtsanwältinnen und Rechtsanwälten sowie der Rechtsanwaltskammer Frankfurt am Main wurde allerdings zunehmend deutlich, dass diese sich im Rahmen ihrer anwaltlichen Tätigkeit nicht zwangsläufig als datenverarbeitende Stelle verstehen, jedenfalls die Anwendbarkeit des BDSG und somit auch meine aufsichtsbehördliche Tätigkeit im Wesentlichen in Frage stellten. Dies u. a. mit der Begründung, dass Regelungen der Bundesrechtsanwaltsordnung (BRAO) als bereichsspezifische Normen gegenüber den Datenschutzregelungen vorrangig seien.

5.5.1.1.1
Das Verhältnis von BDSG und BRAO

Richtig ist, dass andere Rechtsvorschriften zum Umgang mit personenbezogenen Daten grundsätzlich gemäß § 1 Abs. 3 S. 1 BDSG gegenüber den Regelungen des BDSG vorrangig sind.

§ 1 Abs. 3 S. 1 BDSG

Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

Allerdings betrifft der Vorrang anderer Normen nur solche Regelungen, die auch tatsächlich einen datenschutzrechtlichen Bezug aufweisen. Somit sind zwar die Regelungen der BRAO für die inhaltliche Beurteilung des berufsrechtlichen Verhaltens von Rechtsanwältinnen und Rechtsanwälten einschlägig. Für die automatisierte Datenverarbeitung sowie die Verarbeitung von personenbezogenen Daten mit Dateibezug ist mangels bereichsspezifischer Regelungen in der BRAO jedoch weiterhin das BDSG anwendbar.

Darüber hinaus führt der Vorrang anderer Rechtsnormen außerhalb des BDSG auch nicht dazu, dass ich als Aufsichtsbehörde nicht mehr kontrollbefugt bin. Gemäß § 24 Abs. 1 HDSG überwacht der Hessische Datenschutzbeauftragte die Einhaltung der Vorschriften des HDSG sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen. Mein Aufgabenbereich erstreckt sich somit auf alle Regelungen mit datenschutzrechtlichem Bezug.

5.5.1.1.2
Grenze des BDSG

Die Grenze meiner aufsichtsbehördlichen Tätigkeit gegenüber der Rechtsanwaltschaft ist ungeachtet des vorher Gesagten jedoch immer dann er-

reicht, wenn die Verschwiegenheitspflicht aus dem Mandantenverhältnis greift. Dies ergibt sich aus § 1 Abs. 3 S. 2 BDSG.

§ 1 Abs. 3 S. 2 BDSG

Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleiben unberührt.

Hierdurch ist sichergestellt, dass durch das BDSG bereichsspezifisch garantierte Geheimhaltungspflichten bestimmter Berufsgruppen, die elementar für das Vertrauensverhältnis zwischen dem Bürger und der jeweiligen Berufsgruppe sind, nicht ausgehebelt werden. Jedoch nicht für alle spezifischen Geheimhaltungspflichten ist das Spannungsverhältnis zum BDSG einheitlich aufzulösen.

Die Besonderheit beim Anwaltsgeheimnis liegt in der Rolle der Rechtsanwälte als Interessenvertreter ihrer Mandanten. Dies ist ausdrücklich auf die Wahrung oder Durchsetzung von Rechten gegenüber Dritten gerichtet. Im Rahmen eines Rechtsstreits soll der Gegner nur die Informationen erhalten, die der Mandant selbst preisgeben will. Dadurch wird z. B. verhindert, dass ein Prozessgegner im Wege des Auskunftsrechts nach § 34 BDSG die Rechtsanwältin oder den Rechtsanwalt des anderen aushorchen kann.

Soweit eine Fragestellung den Bereich des anwaltlichen Mandantengeheimnisses betrifft, sind vor diesem Hintergrund auch die aufsichtsbehördlichen Überprüfungsmöglichkeiten begrenzt. Dies zeigt sich insbesondere im Umgang mit der mir gegenüber obliegenden Auskunftspflicht nach § 38 Abs. 3 BDSG.

§ 38 Abs. 3 S. 1 BDSG

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen.

Grundsätzlich sind alle datenverarbeitenden Stellen nach § 38 Abs. 3 S. 1 BDSG verpflichtet, die Fragen des Hessischen Datenschutzbeauftragten zu beantworten und entsprechende Stellungnahmen abzugeben. Ausgenommen sind nach § 38 Abs. 3 S. 2 BDSG nur die Auskünfte auf solche Fragen, deren Beantwortung den Auskunftspflichtigen selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Ordnungswidrigkeitenverfahrens aussetzen würde.

Somit sind grundsätzlich auch Rechtsanwältinnen und Rechtsanwälte als jeweils datenverarbeitende, nicht-öffentliche Stelle im Sinne des BDSG ebenso über § 38 Abs. 3 S. 1 BDSG zur Auskunft gegenüber dem Hessischen Datenschutzbeauftragten verpflichtet.

Dem steht jedoch die berufliche Verschwiegenheitspflicht entgegen, die sich konkret aus § 43a Abs. 2 BRAO und § 203 Abs. 1 Nr. 3 des StGB ergibt. Es handelt sich um eine der anwaltlichen Grundpflichten.

§ 43a Abs. 2 BRAO

Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

§ 203 Abs. 1 Nr. 3 StGB

Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

…

3. Rechtsanwalt, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

...

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Es besteht also ein Spannungsverhältnis zwischen der Auskunftspflicht nach § 38 Abs. 3 BDSG einerseits und der Verschwiegenheitspflicht aufgrund des Mandatsgeheimnisses andererseits. Da jedoch der Schutz von Daten Dritter und der Umgang mit diesen Daten durch Rechtsanwältinnen und Rechtsanwälte auch grundsätzlich von § 1 Abs. 1 BDSG erfasst ist, reicht mein Auskunftsrecht ihnen gegenüber zumindest so weit, dass eine Einschätzung möglich ist, ob im jeweiligen Fall das Mandantengeheimnis überhaupt greift oder nicht.

Im Rahmen eines Auskunftsverlangens nach § 38 Abs. 3 BDSG muss daher stets einzelfallbezogen anhand der Informationen des Eingebers und der Stellungnahme der jeweiligen Rechtsanwältin oder des jeweiligen Rechtsanwalts geprüft werden, ob der Bereich des Mandantengeheimnisses betroffen ist oder nicht und daher eine Verpflichtung zur Auskunft besteht oder nicht.

5.5.1.2
Konsequenzen für die Praxis

5.5.1.2.1
Textverarbeitung ist automatisierte Datenverarbeitung

Im Rahmen einer Eingabe ging es u. a. um die Fragestellung, ob ein Datenverarbeitungsvorgang im Sinne des BDSG bei einer bestimmten anwaltlichen Tätigkeit überhaupt vorliegt. Ein Bürger hatte ein als Informationsschreiben bezeichnetes Schriftstück einer Rechtsanwaltskanzlei im Zusammenhang mit möglichen Rückforderungsansprüchen bei Verbraucherdarlehen erhalten. Unklar war, wie die Kanzlei in diesem Kontext an die Privatanschrift des Bürgers gekommen war und ihn in diesem Zusammenhang angeschrieben hatte, so dass ich mich mit der Bitte um entsprechende Auskunft an die Kanzlei wandte. Die Kanzlei teilte daraufhin mit, dass es sich um ein Informationsschreiben gehandelt habe und die Adresse dem Telefonbuch entnommen worden sei. Darüber hinaus handele es sich nach Auffassung der Kanzlei aber weder um eine automatisierte Verarbeitung personenbezogener Daten noch um eine Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien.

Bei Adressdaten aus dem Telefonbuch handelt es sich durchaus um Daten, die allgemein zugänglich sind und daher im Sinne von § 28 Abs. 1 Nr. 3 BDSG zulässigerweise erhoben und für eigene Geschäftszwecke genutzt werden dürfen. Unter datenschutzrechtlichen Gesichtspunkten bestanden daher in diesem Punkt vorerst keine weitergehenden Bedenken gegen den Erhebungs- und Nutzungsvorgang durch die Kanzlei.

Allerdings war die Einschätzung der Kanzlei, dass es sich hier nicht um eine Datenverarbeitung handele, unzutreffend. Ich erlaubte mir daher den ergänzenden Hinweis gegenüber der Kanzlei, dass es sich in diesem Fall durchaus um eine automatisierte Datenverarbeitung im Sinne des BDSG handelte. Denn gemäß § 3 Abs. 2 BDSG ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen eine automatisierte Datenverarbeitung im Sinne des BDSG.

§ 3 Abs. 2 BDSG

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Hierunter fallen insbesondere auch Texte in Textverarbeitungssystemen. Alle computertechnisch gestützten Textverarbeitungsvorgänge im Rahmen anwaltlicher Tätigkeit, wie z. B. das Anfertigen von Schriftstücken auf dem Computer, stellen also eine automatisierte Datenverarbeitung im Sinne des BDSG dar, so dass hier datenschutzrechtliche Vorgaben auch für die Rechtsanwaltschaft entsprechende Berücksichtigung finden müssen.

5.5.1.2.2
Auskunftspflicht gemäß § 38 Abs. 3 BDSG vs. Mandatsgeheimnis

Die Frage, ob eine Auskunftspflicht nach § 38 Abs. 3 BDSG besteht oder die Verschwiegenheitspflicht aus dem Mandatsverhältnis greift, betraf weitere Eingaben, die jeweils jedoch unterschiedlich zu bewerten waren.

5.5.1.2.2.1
Begrenzte Auskunftspflicht

In einem Fall vertrat ein Rechtsanwalt eine Gläubigergesellschaft. Im Rahmen seiner anwaltlichen Tätigkeit wandte er sich sowohl per Post als auch per E-Mail an potenzielle Drittschuldner seiner Mandantschaft. Das anwaltliche E-Mail-Schreiben war zudem an einen offenen Verteiler versandt worden, so dass für alle angeschriebenen Personen auch alle anderen Empfänger erkennbar waren.

Fraglich war zunächst, wie der Rechtsanwalt an alle Anschriften und E-Mail-Adressen der möglichen Drittschuldner gekommen war. Einzelne Adressaten dieser Schreiben hatten sich daher mit einem Auskunftsersuchen nach § 34 Abs. 1 BDSG an den Rechtsanwalt gewandt, um die Hintergründe in Erfahrung zu bringen. Da eine Auskunft seitens des Rechtsanwalts insofern jedoch nicht erteilt wurde, wandten sich die Betroffenen an mich. Auf mein Auskunftsersuchen hin verwies der Rechtsanwalt unter Bezugnahme auf das Urteil des Kammergerichts Berlin vom 20. August 2010 (Az. 2 Ss 23/07) zunächst vollumfänglich auf die anwaltliche Verschwiegenheitspflicht.

Wie bereits aufgezeigt, reicht mein Auskunftsrecht gegenüber Rechtsanwältinnen und Rechtsanwälten zumindest so weit, dass ich einschätzen kann, ob im jeweiligen Fall das Mandantengeheimnis betroffen ist oder nicht.

Entsprechend teilte ich dies dem Rechtsanwalt in diesem Fall daher auch ergänzend mit. Daraufhin erklärte der Rechtsanwalt schließlich, dass er die Daten anonym erhalten habe. Mit dieser Erklärung war der Rechtsanwalt seiner Auskunftspflicht nach § 38 Abs. 3 BDSG aber auch bereits umfäng-

lich nachgekommen. Da es mir nicht erlaubt ist, Einsicht in die Mandatsakten zu nehmen, war eine weitere Überprüfung zur Herkunft der Adressdaten für mich als Aufsichtsbehörde leider nicht möglich. An diesem Punkt war die Grenze der Auskunftspflicht und meiner Kontrollbefugnis erreicht.

Im Hinblick auf die Tatsache, dass die E-Mail-Schreiben an einen offenen Verteiler versandt wurden, hatte ich den Rechtsanwalt in meinem Auskunftsersuchen bereits darauf hingewiesen, dass es sich um eine unberechtigte Datenweitergabe handelte, die grundsätzlich sogar den Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG erfüllt. Der Rechtsanwalt übernahm hierfür die Verantwortung, entschuldigte sich und teilte mit, dass es sich um einen technischen Fehler gehandelt habe und der entsprechende E-Mail-Account sowie sämtliche E-Mail-Adressen gelöscht wurden.

5.5.1.2.2.2
Mandatsgeheimnis nicht betroffen

In einem anderen Fall beschwerte sich ein Bürger bei mir, dass die gegnerische Rechtsanwältin, die im Rahmen eines Scheidungsverfahrens seine Exfrau anwaltlich vertrat, gegenüber seinem Energieversorger die Änderung seiner Adressdaten mitgeteilt habe. Aufgrund der mir vom Bürger mitgeteilten Umstände wandte ich mich daher an die Rechtsanwältin und bat um entsprechende Auskunft, aufgrund welcher Informationen und auf welcher Rechtsgrundlage eine Adressänderung für den Bürger, der immerhin nicht ihr Mandant war, beim Energieversorger durch sie vorgenommen wurde und ob auch noch weitere Adressänderungen für ihn durch sie vorgenommen worden seien. Im Rahmen ihrer ersten Stellungnahme verwies die Rechtsanwältin im Wesentlichen auf ihre anwaltliche Schweigepflicht. Darüber hinaus verwies sie darauf, dass die Mitteilung ladungsfähiger Anschriften zu ihrer Aufgabe als Rechtsanwältin gehöre und die derzeitige Aufenthaltsanschrift des Eingebers von diesem auch selbst im Rahmen einer Gerichtsverhandlung mitgeteilt worden sei.

Der Verweis auf die anwaltliche Schweigepflicht war in diesem Kontext jedoch verfehlt, da es hier um die Weitergabe von personenbezogenen Daten eines anderen, der nicht ihr Mandant war, an einen Dritten, nämlich den Energieversorger, ging. Des Weiteren war aufgrund der Stellungnahme der Rechtsanwältin auch nicht erkennbar, warum in diesem Kontext eine Verpflichtung für sie bestanden haben sollte, eine ladungsfähige Anschrift an den Energieversorger mitzuteilen. Eine unter diesem Hinweis ergänzende Aufforderung zur Stellungnahme blieb seitens der Rechtsanwältin jedoch unbeantwortet. Erst nach Androhung eines Zwangsgeldes erhielt ich

schließlich eine Stellungnahme, aufgrund derer mir eine datenschutzrechtliche Einschätzung über die Frage der Zulässigkeit der Weitergabe der Anschriftendaten des Bürgers möglich war.

Dabei kam ich zu dem Ergebnis, dass in der Übermittlung der Anschriftendaten an den Energieversorger zwar grundsätzlich eine unbefugte Weitergabe von personenbezogenen Daten gesehen werden konnte. Denn das Übermitteln von personenbezogenen Daten ist gemäß § 3 Abs. 4 Nr. 3 Buchst. a BDSG das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden. Soweit es sich nicht um eine Verarbeitung im Sinne des § 3 Abs. 4 BDSG handelt, ist das Übermitteln von personenbezogenen Daten jedenfalls eine Nutzung im Sinne von § 3 Abs. 5 BDSG. Die Zulässigkeit einer solchen Datenverarbeitung und -nutzung ergibt sich wiederum aus § 4 BDSG. Sie ist gemäß § 4 Abs. 1 BDSG nur dann erlaubt, soweit ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Aus der letzten Stellungnahme der Rechtsanwältin ergab sich jedoch für mich, dass Hintergrund der Mitteilung an den Energieversorger eine drohende Stromsperre in der von ihrer Mandantin rechtmäßig bewohnten, jedoch noch im Eigentum des Eingebers stehenden Ehewohnung wegen unbezahlter Rechnungen zu befürchten gewesen wäre. Die Mitteilung an den Energieversorger war daher als berechtigte Wahrnehmung von Mandanteninteressen im Rahmen des Scheidungsverfahrens zu werten, welches zur Pflichtaufgabe der Rechtsanwältin gehörte. Denn aus dem Recht zur Beratung und Vertretung (§ 3 Abs. 2 BRAO) und der Pflicht, keine widerstreitenden Interessen zu vertreten (§ 43a Abs. 4 BRAO), folgt zugleich die Pflicht zur Wahrnehmung von Mandanteninteressen. Vor diesem Hintergrund bestanden daher im Ergebnis keine datenschutzrechtlichen Bedenken gegen die Anschriftenmitteilung an den Energieversorger.

5.5.2
Namentliche Nennung von Hausbesitzern auf der Webseite eines Handwerksbetriebes

Die namentliche Nennung von privaten Kunden als Referenzen auf der Webseite eines Unternehmens ist nur mit einer ausdrücklichen Einwilligung der betroffenen Kunden zulässig. Wurden keine Einwilligungen eingeholt, können zwar erfolgreiche Projekte des Unternehmens zu Werbezwecken veröffentlicht werden, jedoch nur, wenn die Angaben anonym und die privaten Kunden bzw. Auftraggeber nicht identifizierbar sind.

Mich erreichte die Beschwerde eines Hausbesitzers, der Angaben über sich und sein Haus auf der Webseite eines nordhessischen Handwerksbetriebs gefunden hatte. Der Betrieb war vor längerer Zeit mit der Installation von Haustechnik in das Haus des Betroffenen beauftragt gewesen. Bei der Überprüfung der Webseite stellte sich heraus, dass dort unter dem Stichwort „Referenzen" Informationen über eine Vielzahl von Gebäuden in der Umgebung zu finden waren, in die der Betrieb erfolgreich verschiedene Anlagen eingebaut hatte. Dabei wurden zu jedem Gebäude nicht nur die technischen Daten der jeweils eingebauten Anlagen, sondern auch der Name des Hausbesitzers, die Anzahl der im Haus wohnenden Personen und der Ortsname, in dem sich das jeweilige Gebäude befindet, angegeben. Die meisten Einträge waren zudem mit Fotos der Häuser und teilweise auch der installierten Anlagen bebildert. Anhand dieser Angaben und Fotos war ohne erheblichen Aufwand eine eindeutige Identifikation fast aller Hausbesitzer bzw. -bewohner möglich.

Als der Handwerksbetrieb mit dieser Tatsache konfrontiert wurde, stellte sich heraus, dass dort bisher keinerlei Bewusstsein für die datenschutzrechtliche Problematik dieser Veröffentlichung bestand. Mit den Namen der Betroffenen und den weiteren identifizierenden Angaben hatte der Betrieb jedoch eindeutig personenbezogene Daten veröffentlicht. Nur wenige der betroffenen Kunden des Betriebs hatten aber der Veröffentlichung ihrer Daten bewusst zugestimmt. Zwar waren einige der Betroffenen über die Veröffentlichung informiert und damit wohl auch einverstanden, eine ausdrückliche und schriftliche Einwilligung, die den Anforderungen aus § 4a Abs. 1 BDSG entsprach, gab es jedoch in keinem Fall.

§ 4a Abs. 1 BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Zudem wussten viele Hausbesitzer gar nichts von der Veröffentlichung ihrer Daten auf der Webseite des Handwerkers.

Ohne eine Einwilligung der Betroffenen ist die Veröffentlichung der Referenzen in der vom Handwerksbetrieb gewählten Form aber nicht zulässig. Der Zweck der Veröffentlichung, mit erfolgreichen Bauprojekten zu werben, kann auch ohne die namentliche bzw. identifizierende Nennung der bishe-

rigen Privatkunden verfolgt werden. Im Gegensatz zur Nennung von bedeutenden und bekannten Kunden wie z. B. Großunternehmen oder Behörden, deren Namen als Referenzen dienen, ist es bei der Werbung mit Tätigkeiten bei privaten Kunden weder erforderlich noch nützlich, deren Namen zu nennen.

Der Betrieb wurde von mir aufgefordert, entweder die identifizierenden Angaben von der Webseite zu entfernen oder schriftliche Einwilligungen zur Veröffentlichung der Daten von allen betroffenen Personen einzuholen. Daraufhin wurden die Namen der Betroffenen sowie die Angaben über die Anzahl der Bewohner der Häuser von der Webseite entfernt. Die nunmehr auf der Webseite noch vorhandenen technischen Daten der installierten Anlagen und die Information, in welchen Orten diese verbaut wurden, lassen keinen direkten Bezug zu bestimmten oder bestimmbaren Personen mehr zu und stellen somit keine personenbezogenen Daten mehr dar. Auf diese Weise kann der Betrieb weiterhin mit seinen bisherigen Tätigkeiten werben, ohne dass dadurch die Persönlichkeitsrechte seiner Kunden in Mitleidenschaft gezogen werden.

5.5.3
Ausgestaltung von Verlagsumfragebogen

Anlässlich einer Eingabe habe ich mich mit der Ausgestaltung von Verlagsumfragebogen beschäftigt. Aufgrund meiner Kritik wurden die den Lesern mitgeteilten Informationen über die weitere Verarbeitung ihrer Antworten präzisiert und mehr Transparenz für die Befragten hergestellt.

5.5.3.1
Der Anlass

Die mit der Eingabe vorgetragenen Bedenken bezogen sich auf einen Fragebogen einer überregionalen Tageszeitung zur Wahl 2013. Gefragt war die Meinung der Leser zu einzelnen Themen aus den Bereichen Innenpolitik, Außenpolitik, Wirtschaftspolitik sowie zu sozialpolitischen Themen. Eine Frage aus dem Bereich der Innenpolitik lautete beispielsweise: „Die FDP ist bei der Bundestagswahl zum ersten Mal an der Fünfprozenthürde gescheitert. Glauben Sie, dass die FDP vom Wähler auch bei den drei Landtagswahlen 2014 abgestraft wird?“

Der Fragebogen enthielt den Hinweis: „Die Auswertung erfolgt anonym.“ Zugleich war jedoch auf der Rückseite ein Freitextfeld für die persönliche Anschrift gegeben, mit der man sich für ein Abonnement inklusive Gewinn-

spiel anmelden konnte. Damit befanden sich persönliche Daten und zu anonymisierende Daten auf einem Formular.

Wie mir der Verlag auf meine Nachfrage mitteilte, wurden die personenbezogenen Daten und die Antworten auf dem Umfragebogen innerhalb des Verlages technisch und organisatorisch getrennt voneinander erfasst und bearbeitet.

5.5.3.2 Rechtliche Bewertung

Im konkreten Fall erfolgte erst nach Eingang der Daten beim Verlag eine Trennung der Antworten auf dem Umfragebogen und der personenbezogenen Bestelldaten. Beides ist jedoch möglichst auf unterschiedlichen Wegen zu erheben. In jedem Fall ist ansonsten eine Information an die Teilnehmer, dass ihre Antworten bei Eingang ihrer Person zugeordnet werden können, zwingend erforderlich.

Wie aus dem vorliegenden Muster hervorging, wurde eine „anonyme" Auswertung des Fragebogens zugesichert. Diese Begrifflichkeit ist jedoch im gegebenen Fall nicht zutreffend, da die zu trennenden Daten bei derselben Daten verarbeitenden Stelle eingehen und daher ohne weiteres einander zuzuordnen sind. Korrekterweise ist hier von einer internen File-Trennung ab Eingang der Daten zu sprechen. Eine File-Trennung stellt eine interne Datensicherheitsmaßnahme dar. Sie führt nicht dazu, dass die Befragung als „anonym" bezeichnet werden kann. Auch in diesem Fall ist es erforderlich, den Teilnehmern an der Umfrage weitere Informationen zum organisatorischen und technischen Ablauf zu geben.

5.5.3.3 Ergebnis

Der beanstandete Verlagsumfragebogen wurde aufgrund meiner Hinweise im Hinblick auf Text und Gestaltung überarbeitet. Insbesondere wird die Verlagsumfrage nunmehr nicht mehr als „anonym" bezeichnet. Der Fragebogen enthält vielmehr den Hinweis, dass die Antworten bei Eingang der Person zuzuordnen sind, die Erfassung und Bearbeitung der personenbezogenen Daten und der Antworten auf dem Umfragebogen jedoch „technisch und organisatorisch" getrennt erfolgen.

Zudem besteht für den Teilnehmer jetzt die Möglichkeit, den Fragebogen und das Abonnement vor der Einsendung voneinander zu trennen. Die Möglichkeit der Trennung von Fragebogen und Abonnement ist demnach

noch einmal optisch hervorgehoben worden. Hier empfiehlt sich die Verwendung eines Scherensymbols o. Ä. Die Antworten sind damit zwar nach wie vor bei Eingang der teilnehmenden Person zuzuordnen, es wurde mir jedoch noch einmal versichert, dass die Erfassung und Bearbeitung der personenbezogenen Daten und der Antworten technisch und organisatorisch getrennt erfolgen. Da die Hinweise auf dem neu gestalteten Verlagsumfragebogen die Teilnehmer hierüber auch entsprechend aufklären, bestanden bei mir keine weiteren Bedenken.

5.6
Gesundheitswesen

5.6.1
Verwendung von Adressdaten zu Werbezwecken in Apotheken

Viele Apothekenkunden erhalten mittlerweile in regelmäßigen Abständen Post aus ihrer Apotheke. Das Versenden von Werbeanschreiben ist auch für Apotheken ein beliebtes Marketinginstrument zur Stärkung der Kundenbindung geworden. Eine Eingabe eines Apothekenkunden habe ich zum Anlass genommen, mich mit den Voraussetzungen, Zulässigkeit und dem Verfahren beim Versand von solchen Schreiben zu befassen.

5.6.1.1
Post aus der Apotheke

Im vorliegenden Fall versendete eine hessische Apotheke mehrmals im Jahr Briefe an ihre „langjährigen, treuen“ Kunden. Die Liste mit den Adressen der angeschriebenen Kunden wurde seit vielen Jahren über die Rückmeldungen der Kunden im Rahmen von Gewinnspielen und direkter Kundenansprache in der Apotheke gepflegt und aktualisiert. Eine ehemalige Kundin der Apotheke bat mich um Überprüfung der Verfahrensweise und trug mir gegenüber vor, sie hätte nie eine Einwilligung für die Aufnahme in der Kundenkartei erteilt.

5.6.1.2
Datenschutzrechtliche Bewertung

Nach den gesetzlichen Bestimmungen über den Datenschutz und nach § 2 Abs. 2 der Berufsordnung der Landesapothekerkammer Hessen ist eine Speicherung von Kundendaten durch die Apotheke ohne Einwilligung des

Kunden nicht zulässig, sofern sie nicht nach den gesetzlichen Vorschriften oder anderer Ermächtigungsgrundlagen erlaubt sind oder gefordert werden.

Es gibt im Bundesdatenschutzgesetz nur wenige Ausnahmen, in denen bei Datenerhebung und Speicherung von personenbezogenen Daten auf die Einwilligung verzichtet werden kann. So ist nach § 28 Abs. 1 BDSG das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es zur Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit den Betroffenen erforderlich ist. Ein solcher Fall könnte zum Beispiel sein, dass die Apotheke ein Medikament nicht vorrätig hat und sich die Adresse des Kunden notiert, um ihm das Medikament nachzuliefern. Ein Versand von Werbeschreiben ist jedoch nicht Bestandteil des routinemäßigen Vertrages einer Apotheke mit dem Kunden. Auf diese Regelung kann die Speicherung und Verwendung einer Kundenliste nicht gestützt werden.

Eine weitere Möglichkeit, eine Adressliste ohne eine Einwilligung der Kunden zu nutzen, könnte sich aus den Regelungen zur Verarbeitung von personenbezogenen Daten zum Zwecke der Werbung nach § 28 Abs. 3 BDSG ergeben. In Abs. 3 Satz 1 hat der Gesetzgeber die Verarbeitung oder Nutzung personenbezogener Daten unter einen Einwilligungsvorbehalt der Betroffenen gestellt.

§ 28 Abs. 3 Satz 1 BDSG

Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt.

Die Vorschrift sieht jedoch eine Ausnahme von der Einwilligungserfordernis vor. Für Werbezwecke kann nach § 28 Abs. 3 Satz 2 BDSG die Verarbeitung oder Nutzung listenmäßig oder sonst zusammengefasster Daten einer Personengruppe zulässig sein (sog. Listenprivileg). Die Daten müssen sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken. Werden ausschließlich diese zuvor genannten Daten verwendet, wird für die Speicherung und Nutzung der Kundendaten zum Zwecke der Werbung keine Einwilligung der Betroffenen benötigt.

Klärungsbedürftig ist jedoch, woher die Adressdaten der Apotheke stammen. Die betroffene Apotheke gab mir gegenüber an, dass alle Adressdaten im Rahmen eines Kundenkontaktes erhoben wurden. § 28 Abs. 3 BDSG

gestattet die Verwendung von Daten, die im Rahmen eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses (insbesondere Vertrag, Vertragsverhandlungen) erhoben wurden. Ein Schuldverhältnis liegt auch bei der Einreichung von Rezepten vor. Jedoch ist es für die Rezepteinlösung nicht erforderlich, die Adresse des Kunden zu erheben. Auch wenn auf Rezepten die Kundenadresse vermerkt ist, dürfen diese Daten daher nicht für Werbeschreiben bzw. Erstellung einer Kundenliste verwendet werden. Für die Verwendung zu Werbezwecken kommen daher nur Daten in Betracht, die unabhängig von einer Rezepteinlösung in der Apotheke erhoben wurden. Jedoch wird es bei Kunden, die kein Rezept einlösen, für die Abwicklung des Verkaufsgeschäftes (z. B. Kauf eines Drogerieartikels) im Regelfall nicht erforderlich sein, die Adresse und den Namen des Kunden zu erheben. Somit ergeben sich auch hier nicht automatisch Adressdaten, die für die Werbeschreiben genutzt werden könnten.

Im Ergebnis ist festzustellen, dass eine Nutzung von Adressdaten aus Rezepten für Werbezwecke ausscheidet und auch ein Geschäftsverhältnis außerhalb der Rezepteinlösung zu keiner Erhebung von Adressdaten führt. Es bleibt daher für die Apotheke nur die Möglichkeit, Kundenadressen mit einer schriftlichen Einwilligung der Betroffenen zu erheben. Diese Einwilligungserklärungen sind dann auch aufzubewahren, um nachweisen zu können, dass die Datenbeschaffung und Nutzung rechtmäßig erfolgt ist. Für alle Datensätze, bei denen keine Einwilligung nachweisbar ist, kann nicht belegt werden, dass die Daten zulässig erhoben wurden. Sie dürfen somit nicht verwendet werden und sind zu löschen.

5.6.1.3
Konsequenzen im Einzelfall

Die betroffene Apotheke teilte mir mit, dass sie seit einigen Jahren ihre Kundenliste für Werbeschreiben auf der Basis von schriftlichen Einwilligungserklärungen speichert und verwendet. Die entsprechende Erklärung der Petentin war jedoch nicht mehr auffindbar. Somit mussten die Daten der Petentin aus der Adressdatei gelöscht werden. Ich habe die Apotheke darauf hingewiesen, dass alle Datensätze, für die sie keine entsprechende Einwilligungserklärung vorweisen kann, ebenfalls zu löschen sind.

5.6.2
Aufbewahrung von Rezepten und Patientenüberweisungen in der Arztpraxis

Arztpraxen müssen sicherstellen, dass unbefugte Dritte insbesondere im Empfangsbereich keinen Einblick in Patientenakten nehmen können.

Gelegentlich erhalte ich auch Anfragen von Strafverfolgungsbehörden, die sich erkundigen, ob die Abläufe und Gegebenheiten in einer Arztpraxis mit den datenschutzrechtlichen Anforderungen konform gehen.

Eine Anfrage aus dem letzten Jahr bezog sich im Wesentlichen auf den Fall, dass es sich ein Arzt zur Gewohnheit gemacht hatte, in seiner Praxis für seine Patienten Rezepte und/oder Patientenüberweisungen zur Abholung frei zugänglich am Empfangstresen auszulegen. Beabsichtigt war hiermit offenbar eine „schnelle und unkomplizierte" Patientenversorgung.

Die in diesem Zusammenhang aufgeworfenen Fragen habe ich wie folgt beantwortet:

5.6.2.1
Wie müssen vollständig ausgefüllte Rezepte und Patientenüberweisungen gelagert werden?

Bei Gesundheitsdaten, zu denen auch Rezepte und Patientenüberweisungen gehören, handelt es sich um besondere Arten personenbezogener Daten, d. h. um Daten mit einer erhöhten Schutzbedarfsklasse. Nach den Regelungen in § 9 BDSG i. V. m. der Anlage zu § 9 BDSG ergibt sich daraus bei den in der Arztpraxis zu treffenden technisch-organisatorischen Maßnahmen ein sehr hohes Sicherheitsniveau. Dieses Niveau ist sicherzustellen, auch wenn im Praxisbetrieb oft eine schnelle und unkomplizierte Patientenversorgung gefragt ist. Gerade im Eingangs-/Empfangsbereich ist daher zu gewährleisten, dass unbefugte Dritte weder einen Einblick noch einen Zugriff auf die Patientendaten erhalten. Patientendaten dürfen nicht unbefugt i. S. v. § 203 StGB Dritten offenbart werden. Die Art der Aufbewahrung ist nicht konkret vorgeschrieben. Es muss sich hierbei nicht zwingend um einen Safe handeln. Entsprechende Dokumente sollten jedoch zumindest in verschlossenen Vorrichtungen aufbewahrt werden, sofern kein Personal anwesend ist.

5.6.2.2
Gibt es auch allgemein für Rezepte bezüglich des Datenschutzes entsprechende Rechtsnormen und bei Verstoß gegen die Lagerungsvorschriften tangierte Straf- oder Ordnungswidrigkeitstatbestände?

Spezielle Vorschriften im Hinblick auf Rezepte existieren, neben den speziellen Regelungen nach dem BtMG, nicht. In Betracht zu ziehen sind jedoch neben dem § 203 StGB die Regelungen in den jeweiligen Berufsordnungen für Ärztinnen und Ärzte. Die zuständige Landesärztekammer hat in-

soweit die Möglichkeit, wegen derartiger Verstöße ein berufsrechtliches Verfahren einzuleiten.

5.6.2.3
Entfallen mögliche Datenschutznormen, wenn zuvor der Patient (mündlich am Telefon oder schriftlich) einer öffentlich frei zugänglichen und einsehbaren Lagerung zugestimmt hat?

Es wird hier von der eingangs geschilderten Konstellation ausgegangen. Das heißt, die Frage lautet, ob Patienten darin einwilligen können, dass für sie bestimmte Rezepte und/oder Patientenüberweisungen frei zugänglich am Tresen zur Abholung ausgelegt werden. Eine sogenannte „informierte" Einwilligung ist hier bereits deshalb nicht möglich, da der Personenkreis, der das Rezept/die Überweisung zur Kenntnis nehmen könnte, zu unbestimmt ist. Denkbar ist insoweit immer, dass sich Personen in der Praxis aufhalten bzgl. derer gerade keine Kenntnisnahme gewünscht ist (Arbeitgeber, Nachbar etc.).

5.6.3
Aufzeichnung von Telefonaten aus „Compliance-Gründen"

Auch im Gesundheitsbereich sind Telefon-Hotlines anzutreffen, mittels derer ein Unternehmen den Kunden Informationen zu seinen Produkten zukommen lässt. Besondere Fragen stellen sich hier, wenn die Telefonate zu bestimmten Zwecken aufgezeichnet werden sollen und Gegenstand der Telefonate insbesondere auch die Gesundheit des Anrufers ist.

5.6.3.1
Ausgangslage

Bei dem konkreten Unternehmen, auf das mich ein Petent aufmerksam gemacht hat, handelt es sich um einen Anbieter von Medizinprodukten aus dem Diabetes-Segment. Sofern deren kostenfreie 0800er-Nummer angewählt wurde, erhielt der Anrufer zu Beginn die Information vom Band, dass sämtliche Gespräche zu „Qualitäts- und Trainingszwecken" sowie aus „Compliance-Gründen" aufgezeichnet werden. Der Anrufer hatte nicht die Möglichkeit, dem zu widersprechen oder dieses Verfahren zu umgehen.

Auf meine konkrete Nachfrage hierzu teilte mir das Unternehmen mit, dass die Aufzeichnung der Gespräche vor allem aus „Compliance-Gründen" erfolge. Die diesbezüglich zitierte Richtlinie 98/79/EG enthält jedoch keine ausdrückliche gesetzliche Grundlage für das Aufzeichnen von entspre-

chenden Telefonaten im Sinne einer Aufzeichnungspflicht. Derartiges regelt beispielsweise das Hessische Rettungsdienstgesetz (HRDG) in § 17 Abs. 5, in dem es heißt: „Die zentralen Leitstellen sind verpflichtet, alle ein- und ausgehenden Fernmelde- und Funkgespräche auf Tonträger aufzuzeichnen."

Ich habe das Unternehmen daher noch einmal ausdrücklich darauf hingewiesen, dass gemäß § 201 StGB die unbefugte Gesprächsaufzeichnung strafbewehrt ist. Damit war es für mich zugleich unerlässlich, dass dem Anrufer bereits vor Beginn des Gespräches die Option ermöglicht wird, ein Gespräch mit oder ohne Aufzeichnung zu führen.

Aufgrund dieser Vorgaben wurde mir ein alternatives Modell vorgeschlagen. Danach sollte der Anrufer durch eine Bandansage auf die Möglichkeit hingewiesen werden, dem Mitarbeiter bei Gesprächsbeginn mitzuteilen, dass er keine Gesprächsaufzeichnung wünscht. Sofern der Anrufer dies unterlässt, wäre von einer konkludenten Einwilligung zur Aufzeichnung des Gespräches auszugehen.

Da bei Nutzung dieser Hotline regelmäßig Gesundheitsdaten offenbart werden, die zu den besonderen Arten personenbezogener Daten i. S. v. § 3 Abs. 9 BDSG zählen und einem besonderen Schutz unterliegen, habe ich auch bezüglich dieser Praxis datenschutzrechtliche Bedenken geäußert. Das alternativ vorgeschlagene Modell wäre z. B. bei der Hotline einer Kfz-Werkstatt denkbar, bei der in der Regel keine sensitiven Daten mitgeteilt werden.

Die Sachlage ist hier jedoch anders. Bereits in den ersten Sekunden des Gespräches gibt der Anrufer möglicherweise detaillierte Angaben zu seiner Gesundheit preis. Dies kann theoretisch dazu führen, dass er von seiner Widerspruchsmöglichkeit absieht, da er davon ausgeht, dass bereits wesentliche Informationen aufgezeichnet wurden.

Eine aus datenschutzrechtlicher Sicht „sichere" Lösung für beide Seiten kann in dieser Konstellation meines Erachtens nur gefunden werden, wenn die Deaktivierung der Gesprächsaufzeichnung bereits vor dem tatsächlichen Beginn des Gespräches erfolgt und nicht während des Gespräches. Auch für das jeweilige Unternehmen besteht dadurch eine wesentlich größere Sicherheit, was eventuelle spätere Einwände von Nutzern der Hotline betrifft (Widerspruch vergessen, indirekt geäußert etc.).

5.6.3.2
Ergebnis und Ausblick

Das Unternehmen hat zunächst die Aufzeichnungen eingestellt. Es hat mir mitgeteilt, dass es im Frühjahr 2015 ein neues Verfahren einführen wird, das

meinen Vorgaben entspricht: Der Anrufer wird bereits zu Beginn des Anrufes von einer automatischen Ansage darüber informiert, zu welchen Zwecken man die Gespräche aufzeichnen möchte. Im Anschluss daran wird der Kunde gebeten, seine Zustimmung zu der Aufzeichnung durch das Drücken einer bestimmten Taste (z. B. „1“) zu geben. Gleichzeitig wird dem Anrufer die Möglichkeit gegeben, bei Ablehnung der Aufzeichnung eine andere Taste zu bedienen (z. B. „2“), was zur Folge hat, dass die Aufzeichnung unterbleibt. Sollte keine Reaktion erfolgen (d. h. keine der Tasten bedient werden), wird der Anrufer mit dem Mitarbeiter verbunden, ohne dass eine Aufzeichnung stattfindet.

5.6.4
Prüfung der PVS Büdingen

Die Abrechnung privatärztlicher Leistungen durch externe Abrechnungsstellen ist heutzutage auch in Hessen für eine Vielzahl an Krankenhäusern und Arztpraxen ein gängiges Modell. Um einen genaueren Einblick in die bei den Abrechnungsstellen stattfindenden Vorgänge und Abläufe zu bekommen, habe ich zunächst stichprobenhaft eine Prüfung bei der PVS Büdingen durchgeführt. Die Abläufe waren grundsätzlich datenschutzgerecht gestaltet.

5.6.4.1
Ausgangslage

Die PVS Büdingen ist eine von 14 selbstständigen, privatärztlichen Verrechnungsstellen in Deutschland, die nach eigenen Angaben zusammen einen Marktanteil von ca. 35 % haben. In Konkurrenz hierzu stehen ungefähr 250 gewerbliche Abrechnungsunternehmen in unterschiedlicher Größe und mit abweichenden Marktanteilen.

Im Jahr werden über die PVS Büdingen über zwei Millionen Abrechnungen erstellt.

Anlass für meine Prüfung war der Umstand, dass im letzten Jahr immer häufiger Anfragen von Patienten zu Einwilligungsformularen eingingen, welche die Weiterleitung von Patientendaten zu Abrechnungszwecken an eine Abrechnungsstelle betrafen. Hier ist generell eine informierte Einwilligung zu fordern. Das heißt insbesondere, der Patient muss darüber aufgeklärt werden, an wen, in welchem Umfang und zu welchem Zweck seine Daten weitergegeben werden.

§ 4a BDSG

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Ich habe die Erfahrung gemacht, dass die weiterleitenden Krankenhäuser und Arztpraxen, die für das Einholen der Einwilligungserklärung zuständig sind, gelegentlich nur unzureichend darüber informiert sind, was mit den weitergegebenen Daten bei der PVS geschieht und in welchem Umfang diese dort benötigt und ggf. gespeichert werden.

5.6.4.2
Die Abläufe im Detail

Die PVS Büdingen hat mir die Abläufe der Datenverarbeitung detailliert dargelegt.

5.6.4.2.1
Welche Einwilligungserklärung wird verwendet?

Gegenüber ihren Vertragspartnern weist die PVS auf die Erforderlichkeit einer Einwilligungserklärung hin. Die Ausgestaltung wird jedoch den Vertragspartnern überlassen. Diese können auch auf Muster zugreifen, welche ihnen die jeweilige PVS zur Verfügung stellt.

Nach der Empfehlung der PVS Büdingen sollen die Ärzte regelmäßig die Unterschriften der Patienten erneuern lassen.

5.6.4.2.2

Wie und in welchem Umfang bekommt die PVS Büdingen Daten?

Derzeit erhält die PVS Büdingen die Abrechnungsdaten auf vier verschiedene Arten:

– Online; die Übermittlung erfolgt hierbei über ein Online-Portal. Die Dateien werden beim Hochladen verschlüsselt an die PVS Büdingen übertragen. Dieser Datentransport ist schwerpunktmäßig für Arzt- und Zahnarztpraxen vorgesehen. Die per Datenträger eingehenden Informationen enthalten lediglich die für die Abrechnung erforderlichen Daten, ohne umfassende Behandlungsdokumentation. Als Aufbewahrungsfrist sind zehn Jahre ab dem Rechnungsausgangsdatum vorgesehen. Dies wird mit der notwendigen Beweispflicht der PVS bei eventuellen Rechtsstreitigkeiten begründet.
– Krankenblätter; hierbei handelt es sich im Regelfall um komplette Patientenakten aus den Krankenhäusern oder einzelnen Arztpraxen. Die PVS bedient sich hier neben einem Kurierdienst auch eines eigenen Kurierfahrers, der die Akten in verplombten Kisten abholt und auch auf diese Weise sofort nach Rechnungserstellung wieder an die Krankenhäuser zurückliefert. Nach den Angaben der PVS Büdingen werden von den Krankenakten keine Kopien gefertigt.
– Abrechnungsblätter; als Abrechnungsblatt wird der Durchschreibesatz der konkreten Abrechnung bezeichnet. Die darauf enthaltenen Angaben umfassen den Namen, die Versicherung des Patienten und die Nummer nach der Gebührenordnung (GOÄ) für die durchgeführte Maßnahme. Das Original verbleibt beim Arzt, während die Durchschrift an die PVS Büdingen geht. Nach spätestens einem Jahr erfolgt die Vernichtung durch ein darauf spezialisiertes Unternehmen.
– Datenträger (Disketten, USB-Sticks); für Arztpraxen wird auch die Möglichkeit angeboten, die Abrechnungsdaten per Datenträger an die PVS zu übermitteln. Hierbei handelt es sich um einen eingeschränkten Datenumfang, wie er auch auf den Abrechnungsblättern enthalten ist. Die Aufbewahrungsfrist auf den Servern beträgt – wie im Falle der Online-Übertragung – zehn Jahre. Die Datenträger selbst werden nach spätestens zwölf Monaten vernichtet oder, im Falle der USB-Sticks, nach maximal sechs Wochen formatiert und an den Vertragspartner zurückübersandt.

Im Nachgang zu meiner Prüfung habe ich auch noch einmal ein besonderes Augenmerk auf den genauen Umfang der übermittelten Daten gerichtet. Hierzu habe ich mir beispielhaft einzelne Posteingänge vorlegen lassen.

Während die Abrechnungsblätter bereits eine auf die Erstellung der Abrechnung zugeschnittene Auswahl an Daten enthalten, werden bei den Patientenakten aus den Krankenhäusern keine Einschränkungen vorgenommen. Der Verrechnungsstelle wird kurzfristig die komplette Krankenakte zur Verfügung gestellt.

Wie mir seitens der PVS Büdingen hierzu eingehend dargelegt wurde, können sich regelmäßig aus allen Teilen der Krankenakte für die Abrechnung relevante Details ergeben, die die PVS bei der Rechnungserstellung berücksichtigen muss.

5.6.4.2.3
Was passiert, wenn die Abrechnung bestritten wird?

Sofern ein Patient die übersandte Rechnung beanstandet, erfolgt zunächst eine Korrespondenz mit der PVS Büdingen. Hierzu wurde eine Korrespondenzabteilung eingerichtet. Diese korrespondiert ihrerseits mit dem Behandler, um ggf. notwendige Korrekturen zu veranlassen.

Sollte es zu keiner Klärung der Angelegenheit kommen, richtet sich das weitere Vorgehen nach der jeweiligen Vereinbarung mit dem Vertragspartner. Der Regelfall ist hier die Absendung einer Mahnung nach 44 Tagen sowie die Absendung einer zweiten Mahnung nach weiteren 28 Tagen. Nach erneutem Ablauf von 28 Tagen erfolgt auf Wunsch des Vertragspartners die Abgabe des Vorgangs an einen Rechtsanwalt der PVS oder an einen Rechtsanwalt nach Wahl.

Der Behandler bleibt in allen Fällen weiterhin der Forderungsinhaber.

5.6.4.2.4
Rechnungsversand

Wie bereits eingangs erwähnt, beläuft sich der jährliche Versand an Rechnungen bei der PVS Büdingen auf über zwei Millionen. Um eine entsprechende Logistik vor Ort zu bewältigen, fehlen der PVS Büdingen nach eigenen Angaben die räumlichen, finanziellen und personellen Kapazitäten, weshalb man sich für eine Zusammenarbeit mit einem anerkannten Unternehmen entschlossen hat, das auch im Bereich der Steuerberatung entsprechende Aufträge durchführt. Hierbei wird seit dem Jahr 2010 derart verfahren, dass die fertig gestellten Rechnungsdateien über eine verschlüsselte Verbindung aus einem freigegebenen Bereich von dem Vertragspartner „abgeholt“ und dort ausgedruckt und versandt werden.

5.6.4.2.5
Wie erfolgt der Online-Versand von Abrechnungsdaten?

Der Online-Versand von Abrechnungsdaten wird bei den Ärzten über die Webanwendung „Doc_control“ abgewickelt. Das Programm „Doc_control“ ermöglicht eine gesicherte Übertragung von Daten zwischen dem Arzt und der PVS. Der Zugang in der jeweiligen Arztpraxis ist nur über eine Kennung und ein Passwort möglich. Künftig soll der Zugang nur mit einer zusätzlichen TAN-Nummer möglich sein.

5.6.4.2.6
Können meine Daten auch gelöscht werden?

Unter Ziff. 5.6.4.2.2 wurden bereits die Aufbewahrungsfristen für die bei der PVS Büdingen angelegten Dokumente aufgeführt. Häufig wird die Frage gestellt, ob auch noch nachträglich, das heißt nach vorheriger Zustimmung zur Weiterleitung an die ärztliche Verrechnungsstelle, eine Löschung von Daten vom Patienten verlangt werden kann.

Die verwendeten Mustereinwilligungen sehen grundsätzlich die Möglichkeit vor, die einmal erteilte Einwilligung zu widerrufen. Bei einem Widerruf werden lediglich für die Zukunft keine neuen Daten übermittelt. Die für die Vergangenheit angelegten Daten müssen jedoch immer dann bei der ärztlichen Verrechnungsstelle verbleiben, wenn diese die Rechnungen für den Arzt aufbewahrt.

Anders ist dies lediglich dann, wenn der Patient vorträgt, nie eine Einwilligungserklärung betreffend die Weiterleitung der Daten an die Verrechnungsstelle unterschrieben zu haben. Sollte nichts Gegenteiliges vom Arzt bewiesen werden können, greift ein spezielles Löschprozedere, mit dem alle bei der PVS Büdingen gespeicherten Daten über den Patienten gelöscht werden.

5.6.4.3
Ergebnis der Begehung vor Ort

Bei meiner Begehung habe ich die folgenden Arbeitsbereiche geprüft: Eingangsverwaltung, Archiv, Bereich der Sachbearbeitung, IT-Bereich/Serverraum. Die angetroffenen Abläufe waren grundsätzlich datenschutzgerecht gestaltet.

Die Beanstandungen vor Ort betrafen in erster Linie den Archivbereich. Dort gab es in geringem Umfang Verbesserungsbedarf. Ebenso waren in den verschlossenen Kellerräumen noch Akten gelagert, die gemäß den

vorgesehenen Aufbewahrungsfristen bereits zu vernichten gewesen wären. Bereits kurze Zeit nach meinem Besuch wurden diese Defizite behoben.

Soweit dies den Bereich der Sachbearbeitung betrifft, wurde darauf hingewiesen, dass eine Aktivierungsmöglichkeit von USB-Ports und anderen Datenlese- und Datenübertragungsgeräten nur an den Rechnern vorzusehen ist, an denen dies auch zwingend erforderlich ist. Diese Vorgabe wurde zwischenzeitlich umgesetzt.

Im Nachgang zu der Prüfung habe ich mich noch einmal ausführlich mit der Frage befasst, ob der PVS Büdingen bei der Kundengruppe Krankenhaus tatsächlich die gesamte Krankenakte zur Verfügung gestellt werden muss. Vor dem Hintergrund des Grundsatzes der Datensparsamkeit, der auch bei der Übermittlung von Daten an die Abrechnungsstelle zu berücksichtigen ist, war dies für mich diskussionsbedürftig.

Zu dieser Thematik habe ich folglich noch einmal gesondert Gespräche mit Vertretern der PVS Büdingen geführt. Hierbei wurde mir anhand von konkreten Behandlungsfällen dargelegt, dass insbesondere die komplexen Behandlungsabläufe, die während einer stationären Behandlung stattfinden, eine umfassende Akteneinsicht durch die PVS erforderlich machen, damit eine korrekte und vollständige Rechnung erstellt werden kann. Zugleich konnte übereinstimmend festgehalten werden, dass im Falle von ambulanten Behandlungen die Übersendung der kompletten Patientenakte verzichtbar ist. Es wurde daher vereinbart, dass die PVS ihren Vertragspartnern ein differenziertes Vorgehen vorschlägt.

Ebenso ist es aus meiner Sicht unabdingbar, dass die Patienten im Wege einer informierten Einwilligung darüber in Kenntnis gesetzt werden, dass ihre Krankenakte – zu den im Einzelnen anzuführenden Zwecken – im Falle einer stationären Behandlung „vollständig“ an die PVS Büdingen übergeben wird. Sollte hier bislang in der Einwilligungserklärung nur ein „notwendiger“, „dienlicher“ oder auch „erforderlicher“ Umfang genannt gewesen sein, war dies meines Erachtens nicht dazu geeignet, sich von diesem Umstand eine entsprechende Vorstellung zu machen.

Die PVS Büdingen hat ihre Muster für die Einwilligungserklärung für die Vertragspartner Krankenhaus inzwischen entsprechend umgestellt.

Den Vertragspartnern wurde darüber hinaus durch die PVS noch einmal in einem Anschreiben nahegelegt, sich für die Zukunft Wege zu überlegen, ob und wie der an die Abrechnungsstellen zu übermittelnde Datenumfang weiter eingeschränkt werden kann.

5.7
Versicherungen

5.7.1
Korrespondenz zwischen Versicherung und Versicherungsmakler

Versicherungsunternehmen sind grundsätzlich verpflichtet, auf Verlangen des Versicherungsnehmers mit einem von diesem bevollmächtigten Versicherungsmakler den Schriftwechsel zu führen.

5.7.1.1
Der Anlass

Ein Versicherungsmakler beschwerte sich darüber, dass eine Versicherung Versicherungspolicen und Nachträge zu Versicherungsscheinen – statt an ihn als zuständigen Versicherungsmakler – unzulässigerweise an ein unbeteiligtes Maklerunternehmen sendet.

Konkret gehe es darum, so der Eingeber, dass diese Versicherung (Versicherung A) eine andere Versicherung (Versicherung B) übernommen habe. Er, der Eingeber, sei bisher u. a. Vermittler der Versicherung B gewesen. Infolge der Übernahme sei er nun auch Vermittler der Versicherung A mit eigener Agenturnummer. Für ihn sei nicht nachvollziehbar, dass er von der Versicherung A einem Versicherungsmaklerunternehmen zugeordnet worden sei, mit dem er in keinerlei Verbindung stehe. Er habe schon mehrfach bei der Versicherung A interveniert und dennoch würden weiterhin Versicherungsscheine von seinen Kunden an besagtes Maklerunternehmen gesendet.

Vor diesem Hintergrund nahm ich mit der Versicherung A Kontakt auf. In ihrer Stellungnahme wies diese Versicherung darauf hin, dass ihre Vertriebsverwaltung sich mit der Beschwerde befasst und die Zuordnung des Eingebers zu dem Versicherungsmaklerunternehmen überprüft habe.

Mittlerweile sei die vom Eingeber gerügte Zuordnung aufgehoben worden und für die Zukunft die Beachtung der Agenturnummer des Eingebers sichergestellt, so dass die Versicherung Unterlagen nur noch an die Versicherungsmakleradresse des Eingebers senden werde.

Ich habe den Eingeber in diesem Sinne informiert.

5.7.1.2
Die maßgebende Entscheidung des Bundesgerichtshofs

Mit den bei der Korrespondenz mit Versicherungsmaklern bestehenden Rechtspflichten der Versicherer hat sich auch der BGH grundlegend befasst (Urt. v. 29.5.2013, IV ZR 165/12, NJW 2013, 2354-2357).

Der Versicherungssenat des BGH entschied, dass den Versicherungsunternehmen die vertragliche Nebenpflicht auferlegt ist, auf Verlangen ihrer Versicherungsnehmer mit den von diesen bevollmächtigten Versicherungsmaklern als deren Vertreter die Korrespondenz im Rahmen der Versicherungsverhältnisse zu führen (ebenda Rdnr. 10).

Begrenzt ist diese Verpflichtung der Versicherer, soweit dies im Einzelfall nicht zumutbar ist. Dies können etwa wichtige Gründe in der Person des konkreten Maklers sein, etwa wenn es sich bei dem beauftragten Makler um einen ehemals bei diesem Versicherer beschäftigten Ausschließlichkeitsvertreter handelt. Der Senat weist darauf hin, dass es Versicherern nicht zuzumuten ist, durch Zusammenarbeit mit ehemals eigenen Vertretern deren Geschäftstätigkeit zum möglichen eigenen Nachteil zu fördern (ebenda Rdnr. 16).

Versicherungsnehmer und Makler beschweren sich öfter bei mir, was die Korrespondenz von Versicherern betrifft. Ich fordere deshalb Versicherungen immer wieder auf, die Entscheidung des BGH zu beachten.

5.7.2
Verhinderung von Versicherungsbetrug

Die Verarbeitung von Gesundheitsdaten ist auch ohne Einwilligung des Betroffenen zulässig, wenn es darum geht, Versicherungsbetrug zu verhindern.

5.7.2.1
Der Anlass

Ein Bürger beschwerte sich mit seiner Eingabe über die Versicherung A, bei der er unfallversichert ist.

Nach einem Unfall des Eingebers im Jahr 2011 gab die Versicherung B, mit der er ebenfalls eine Unfallversicherung abgeschlossen hatte, 2012 ein medizinisches Gutachten in Auftrag, das 2013 vorgelegt wurde.

Der Eingeber führte aus, die Aussage des Gutachters, das Gutachten ausschließlich dem Versicherer B zugeleitet, also an keinen anderen Unfallversicherer weitergegeben zu haben, treffe nicht zu. Tatsächlich hätten die Ver-

sicherung B und andere Unfallversicherer, u. a. die Versicherung A, 2012 gemeinsam die Beauftragung eines Gutachters beschlossen und das Gutachten auch erhalten.

Laut der von ihm gegenüber der Versicherung A erteilten Entbindung von der ärztlichen Schweigepflicht im Jahr 2011, so der Eingeber, hätte ihn diese Versicherung darüber informieren müssen, dass sie zusammen mit der Versicherung B das Gutachten in Auftrag geben wolle. Er hätte dann sein Widerspruchsrecht ausüben können. Bislang sei ihm von der Versicherung A jedoch nicht mitgeteilt worden, dass sie das Gutachten mit in Auftrag gegeben habe. Dies, so der Eingeber, sei ein Datenschutzverstoß.

Diese Eingabe gibt Anlass zu folgenden Bemerkungen.

5.7.2.2
Datenschutzrechtliche Bewertung

Der Datenaustausch von Versicherungen bereitet gelegentlich Schwierigkeiten. So rügte ein Eingeber – wie oben beschrieben – das Verhalten einer Versicherung (A). Das Formular dieser Versicherung enthielt für den Eingeber die Information, dass es zur Bewertung der Leistungspflicht des Versicherers erforderlich sein könne, dass die Versicherung Angaben überprüft, die der Versicherungsnehmer zur Begründung seines Anspruchs macht oder die sich aus den von ihm eingereichten Unterlagen ergeben.

Soweit eine solche Überprüfung erforderlich ist, hat der Eingeber die Mitarbeiter der sich aus den vorgelegten Unterlagen ergebenden Stellen und die an der Heilbehandlung Beteiligten von ihrer Schweigepflicht entbunden.

Die Versicherung A verpflichtete sich ihrerseits, ihn vor Erhebung von Daten bei den betreffenden Stellen hierüber zu unterrichten und ihn darauf hinzuweisen, dass er der beabsichtigten Erhebung der Daten widersprechen könne.

Die Versicherung A erhielt im vorliegenden Fall von der Beauftragung des Gutachters allerdings erst 2013, im Zeitpunkt des Erhalts des Gutachtens, Kenntnis, so dass ihr eine vorherige Unterrichtung über eine beabsichtigte Datenerhebung nicht möglich war.

Die Versicherung A hatte 2012 einen Anruf von der Versicherung B und der Versicherung C erhalten und war darüber informiert worden, dass der Eingeber auch mit diesen Versicherungen eine Unfallversicherung abgeschlossen hatte.

Im Rahmen seiner Schadenanzeige bei der Versicherung A hatte der Eingeber nur die Versicherung D als weitere Versicherung benannt. Auch auf seiner 2013 eingereichten Invaliditätsbescheinigung hatte der Eingeber

wider besseren Wissens nur die Versicherung D als weitere Versicherung angegeben und die Versicherung B und die Versicherung C gegenüber der Versicherung A bewusst erneut verschwiegen.

Der Informationsaustausch unter den Versicherungsunternehmen war in der vorliegenden Konstellation ohne Einwilligung des Betroffenen zulässig, weil er dazu diente, in der Gesamthöhe unbegründete Leistungsansprüche abzuwehren. Dies ergibt sich aus § 28 Abs. 6 Nr. 3 BDSG.

§ 28 Abs. 6 Nr. 3 BDSG

Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach § 4a Abs. 3 eingewilligt hat, wenn

...

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

Diese Vorschrift betrifft gerade auch die Fallgestaltung, dass es um Informationen zur Klärung der Berechtigung von Ansprüchen geht, die der Betroffene gegen die Daten verarbeitenden Stellen geltend macht (vgl. bspw. Gola/Schomerus, BDSG, § 28 Rdnr. 78).

In diesem Kontext ist auch die Aufklärung/Aufdeckung von Widersprüchlichkeiten zulässig. Dementsprechend sehen auch die auf § 38a BDSG gestützten Verhaltensregeln der Deutschen Versicherungswirtschaft (Code of Conduct) eine Aufklärung von Widersprüchlichkeiten vor.

Art. 15 Abs. 1 Code of Conduct

Ergeben sich ... nach Vertragsschluss für den Versicherer konkrete Anhaltspunkte dafür, dass ... falsche oder unvollständige Sachverhaltsangaben bei der Feststellung eines entstandenen Schadens gemacht wurden, nimmt das Unternehmen ergänzende Datenerhebungen, -verarbeitungen und -nutzungen vor, soweit dies zur Aufklärung der Widersprüchlichkeiten erforderlich ist.

Zur Sicherstellung einer geordneten Schadenbearbeitung hatte die Versicherung A mit der Versicherung B die Schadenbearbeitung unter deren Federführung vereinbart. Dies schloss auch ein, dass die Versicherung B ein Gutachten in Auftrag gab, die anderen Versicherer das Ergebnis dieses Gutachtens im Rahmen ihrer Schadenbearbeitung ebenfalls berücksichtigen und im Innenverhältnis alle Versicherer anteilig für die Kosten des Gutachtens aufzukommen hätten.

Vor diesem Hintergrund habe ich dem Eingeber mitgeteilt, dass in seiner Angelegenheit ein Datenschutzverstoß nicht vorliegt.

5.8
Vereine, Parteien

5.8.1
Datenschutzprobleme aus der Vereins- und Parteienarbeit

Bei der Vielzahl der in Vereinen, Verbänden und Parteien zu verarbeitenden personenbezogenen Daten von Mitgliedern und Dritten bleiben datenschutzrechtliche Probleme nicht aus. Je nach Größe und Art des Zusammenschlusses gibt es spezifische Besonderheiten, oft aber auch gleichgelagerte Vorfälle und Anfragen.

Hier ein kursorischer Überblick über Eingaben aus dem Berichtsjahr.

5.8.1.1
Personalisierte Essensmarken beim Sportturnier

Der Datenschutzbeauftragte eines hessischen Sportverbandes fragte an, ob es datenschutzrechtlich zulässig sei, Essensmarken für Kampfrichter anlässlich von Turnieren zu personalisieren. Dazu müsste der Sportverband dem Veranstalter eine Liste mit Vor- und Nachnamen der eingesetzten Kampfrichter übermitteln. Der Veranstalter hält die Personalisierung der Essensmarken für erforderlich, weil in der Vergangenheit nie ganz klar war, wer tatsächlich als Kampfrichter eingesetzt war, und deshalb wiederholt Essensmarken auch an Nichtberechtigte ausgegeben wurden, wodurch erhebliche zusätzliche Kosten für den Veranstalter entstanden.

Dem Datenschutzbeauftragten habe ich geantwortet, dass ich es gemäß § 28 Abs. 1 Nr. 2 BDSG für zulässig halte, eine Liste der Kampfrichter (Vor- und Nachname), die an dem geplanten Turnier teilnehmen werden, zu erstellen und diese zwecks Verteilung personalisierter Essensmarken an den Veranstalter zu übermitteln. Die Essensmarken werden in Form eines Wertgutscheins ausgegeben, gelten nur für einen Tag und es werden keine weiteren personenbezogenen Daten in irgendeiner Weise automatisiert gespeichert. Hier besteht meines Erachtens kein Grund zur Annahme, dass schutzwürdige Interessen Betroffener überwiegen. Gleichzeitig wies ich darauf hin, dass die übermittelte Liste nach Durchführung des Turniers wieder ordnungsgemäß gelöscht bzw. vernichtet werden muss.

§ 28 Abs. 1 Nr. 2 BDSG

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, ...*

5.8.1.2
Vorlage einer Personalausweiskopie bei Turnieranmeldung und bei Vereinseintritt

Für die Teilnahme an Wettkämpfen der Landesklasse muss der einzelne Sportler einen sogenannten Startpass beim Bundesverband beantragen. Der Vater einer minderjährigen Tochter beschwerte sich, dass bei der Neuausstellung eines solchen Startpasses unter anderem eine Kopie des Personalausweises eingefordert wurde. Ohne Vorlage dieser Kopie wurde die Ausstellung des Startpasses verweigert.

Dem besorgten Vater habe ich mitgeteilt, dass (sofern das Anfertigen von Personalausweiskopien nicht ausdrücklich – wie beispielsweise im Geldwäsche- oder Telekommunikationsgesetz – zugelassen ist) für das Anfertigen von Kopien von Personalausweis und Reisepass aus sicherheits- und datenschutzrechtlichen Gründen strenge Maßstäbe gelten. Da das Personalausweisgesetz hierzu keine konkreten Vorgaben enthält, hat das Bundesministerium des Innern folgende Rahmenbedingungen formuliert:

- 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.

Der Bundesverband hat mir in seiner Stellungnahme das Erfordernis der Vorlage einer Ausweiskopie nachvollziehbar dargelegt. Es reicht demnach bei der Beantragung eines Startpasses nicht aus, dass allein der Verein (Vereinsbeauftragter) nach Vorlage des Personalausweises die Identität des Sportlers mit Altersangaben und Nationalität bestätigt.

Das Startrecht und der Startpass als „Überprüfungsinstrument" bildet die Grundlage für die Durchführung von fairen Wettkämpfen. Da es immer wieder vorkommt, dass einzelne Vereine Altersangaben oder Nationalität von Sportlern manipulieren, um deren Teilnahme in bestimmte Mannschaften sicherzustellen, ist es erforderlich, den „Pass-Stellen" der Landesverbände eine Kopie des Personalausweises zu übermitteln, damit eine „neutrale" Stelle die Angaben zur Person des Sportlers überprüfen kann. Allerdings waren der Hinweis auf die Möglichkeit der Schwärzung von nicht erforderlichen Daten sowie Art und Weise und Dauer der Speicherung nicht hinreichend geregelt.

Auf meine Intervention hin versicherte mir der Bundesverband, dass er das Antragsverfahren entsprechend der vorstehenden Vorgaben ändern wird. Er wird sicherstellen, dass auf den Ausweiskopien alle nicht erforderlichen Daten geschwärzt werden und dass nach Ausstellung des Startpasses die Pass-Stellen der Landesverbände die vorgelegten Ausweiskopien unter Beachtung datenschutzrechtlicher Vorgaben unverzüglich vernichten.

Zu diesem Thema ging die weitere Beschwerde eines Bürgers ein, weil die Verwertungsgesellschaft Bild und Kunst e.V. für den Abschluss eines Wahrnehmungsvertrages und die damit verbundene Mitgliedschaft die Vorlage einer Kopie des Personalausweises oder Reisepasses verlangte. Die Überprüfung des Sachverhaltes ergab in diesem Fall, dass die Verwertungsgesellschaft Bild und Kunst e.V. die vorstehend aufgeführten strengen Anforderungen zur Kopie von Personalausweis und Reisepass beachtete. Der Vertragsschluss bzw. die Mitgliedschaft erfolgt über den Postweg, der Vertragspartner ist also nicht persönlich anwesend, so dass die Vorlage des Ausweises und die Anfertigung eines Vermerks, dass der Personalausweis vorlag, nicht möglich sind. Die Übersendung der Ausweiskopie erfolgt im Rahmen des Abschlusses des Wahrnehmungsvertrages und der Mitgliedschaft zur Identitätsprüfung. Die Vertragspartner werden von der Verwertungsgesellschaft Bild und Kunst e.V. durch Übersendung eines entsprechenden Merkblattes unterrichtet, dass für die Identitätsprüfung nur Vor-, Nach- und Geburtsnamen sowie eingetragene Künstlernamen, das Geburtsdatum und die Anschrift benötigt werden. Alle anderen Angaben sind

zu schwärzen. Die Ausweiskopie wird nach Überprüfung der Identität sofort nach datenschutzrechtlichen Vorgaben vernichtet. Ein datenschutzrechtlicher Verstoß konnte nicht festgestellt werden.

5.8.1.3
Weitergabe von Daten eines Tierhalters durch Tierschutzverein an einen Geschädigten

Ein Tierheim (Tierschutzverein) schilderte mir folgenden Fall und bat um datenschutzrechtliche Bewertung:

Eine Katze war in ein fremdes Anwesen eingedrungen und hatte die Besitzerin des Anwesens verletzt. Die Katze wurde eingefangen, ins Tierheim verbracht und als „Fundtier" behandelt. Durch den implantierten Chip konnte die Halterin der Katze ermittelt und die Katze dieser zurückgegeben werden. Kurz darauf verlangte der Rechtsanwalt der Geschädigten die Herausgabe der Adressdaten der Halterin zwecks Schadensregulierung. Die Mitarbeiterin des Tierheims war sich unsicher, ob es zulässig sei, die Daten der Halterin an den Rechtsanwalt der Geschädigten herauszugeben. Ich habe ihr mitgeteilt, dass die Übermittlung personenbezogener Daten nach BDSG möglich ist, wenn eine Einwilligung des Betroffenen vorliegt (wovon in dem geschilderten Fall allerdings nicht auszugehen war) oder eine Rechtsgrundlage gegeben ist.

In § 28 Abs. 2 Nr. 2a BDSG ist geregelt, dass im Einzelfall die Übermittlung der Daten, die ursprünglich zu einem anderen Zweck (hier: Versorgung und Rückgabe der Katze) erhoben wurden, zulässig ist, wenn ein berechtigtes Interesse eines Dritten vorliegt und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

§ 28 Abs. 2 Nr. 2a BDSG

Die Übermittlung oder Nutzung für einen anderen Zweck 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 oder Nutzung hat, ...

Die vom Anwalt vorgetragene Begründung der Schadensregulierung stellt ein solches berechtigtes Interesse dar. Ob schutzwürdige Interessen der Halterin der Katze der Übermittlung entgegenstehen, ist vom Tierheim an-

hand der dort bekannten Informationen summarisch zu prüfen und möglichst zu dokumentieren. Dabei kann sich das Tierheim u. a. an der Frage orientieren, welche Konsequenzen die Datenübermittlung für die Halterin haben würde und ob sich daraus ein schutzwürdiges Interesse der Halterin am Ausschluss der Übermittlung ergeben würde.

5.8.1.4
Weitergabe von Mitgliederdaten an ein Vereinsmitglied zur Wahrnehmung satzungsgemäßer Mitgliederrechte

Obwohl einem Kleingartenverein ein rechtskräftiges Urteil vorlag, dass der Verein (vertreten durch seinen Vorstand) verurteilt wird, die derzeit gültige Liste der Mitglieder einschließlich ihrer Anschriften an den Kläger zur Wahrnehmung dessen satzungsgemäßer Minderheitsrechte (§ 37 BGB und entsprechende Paragraphen in der Vereinssatzung) herauszugeben, fragte der Vereinsvorsitzende bei mir an, ob dieses Urteil mit den datenschutzrechtlichen Bestimmungen vereinbar sei.

§ 37 BGB

(1) Die Mitgliederversammlung ist zu berufen, wenn der durch die Satzung bestimmte Teil oder in Ermangelung einer Bestimmung der zehnte Teil der Mitglieder die Berufung schriftlich unter Angabe des Zweckes und der Gründe verlangt.

(2) Wird dem Verlangen nicht entsprochen, so kann das Amtsgericht die Mitglieder, die das Verlangen gestellt haben, zur Berufung der Versammlung ermächtigen; es kann Anordnungen über die Führung des Vorsitzes in der Versammlung treffen. Zuständig ist das Amtsgericht, das für den Bezirk, in dem der Verein seinen Sitz hat, das Vereinsregister führt. Auf die Ermächtigung muss bei der Berufung der Versammlung Bezug genommen werden.

Dem Vereinsvorsitzenden habe ich mitgeteilt, dass der Verein verpflichtet ist, allen Mitgliedern die Ausübung gesetzlicher und satzungsmäßiger Rechte zu ermöglichen. Soweit erforderlich, sind auch die dazu notwendigen Unterlagen, z. B. die Mitgliederlisten, zu übermitteln. Diesem Erfordernis stehen keine schutzwürdigen Interessen der Mitglieder entgegen (§ 28 Abs. 1 Nr. 2 BDSG).

Auch nach Datenschutzrecht ist die Datenübermittlung zulässig. Allerdings empfahl ich dem Vereinsvorsitzenden – um evtl. Missbrauch bei der Verwendung der Daten vorzubeugen – von dem Kläger, dem die Mitgliederdaten ausgehändigt werden sollten, eine schriftliche Erklärung zu verlangen, dass die Adressen nicht für andere Zwecke verwendet werden und sie, sobald sie nicht mehr benötigt werden, datenschutzkonform vernichtet werden.

5.8.1.5
Verpflichtung auf das Datengeheimnis im Verein

Der Vizepräsident (2. Vorsitzender) eines Sportvereins teilte mit, dass vor dem Hintergrund vereinsinterner Querelen der Vereinspräsident (1. Vorsitzender des Sportvereins) den anderen Vorstandsmitgliedern den Zugriff auf die für die Vereinsarbeit notwendigen Mitgliederdaten verweigert, und zwar mit der Begründung, es läge keine Verpflichtung auf das Datengeheimnis gemäß § 5 BDSG der Vorstandsmitglieder vor. Der Vizepräsident bat mich um Auskunft, ob auch die Vorstandsmitglieder nach § 5 BDSG auf das Datengeheimnis zu verpflichten sind. Zu diesem Sachverhalt habe ich folgende Stellungnahme abgegeben:

Nach § 26 BGB wird der Verein gerichtlich und außergerichtlich durch den Vorstand vertreten. Der Vorstand besteht aus mehreren Personen und die Vertretung des Vereins erfolgt durch die Mehrheit der Vorstandsmitglieder.

§ 26 BGB

(1) Der Verein muss einen Vorstand haben. Der Vorstand vertritt den Verein gerichtlich und außergerichtlich; er hat die Stellung eines gesetzlichen Vertreters. Der Umfang der Vertretungsmacht kann durch die Satzung mit Wirkung gegen Dritte beschränkt werden.

(2) Besteht der Vorstand aus mehreren Personen, so wird der Verein durch die Mehrheit der Vorstandsmitglieder vertreten. Ist eine Willenserklärung gegenüber einem Verein abzugeben, so genügt die Abgabe gegenüber einem Mitglied des Vorstands.

Der Verein, vertreten durch die Vorstandsmitglieder, ist verantwortliche Stelle bzw. speichernde Stelle im Sinne des § 3 Abs. 7 BDSG.

§ 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.

Das Bundesdatenschutzgesetz verpflichtet die verantwortliche Stelle (und damit die Vorstandsmitglieder aufgrund ihres Amtes) als Adressat des Gesetzes unmittelbar, die datenschutzrechtlichen Vorschriften zu beachten. Soweit die einzelnen Vorstandsmitglieder für den Verein handeln, müssen sie auf alle erforderlichen Mitgliederdaten zugreifen können, um die ihnen übertragenen Aufgaben ordnungsgemäß zu erfüllen. Sie müssen zudem alle anderen Mitarbeiter, die zum Verein in einem Beschäftigungsverhältnis stehen, und alle sonstigen Personen (auch ehrenamtlich tätige), die mit personenbezogenen Daten des Vereins umgehen, gemäß § 5 BDSG auf das Datengeheimnis verpflichten.

Der Vereinspräsident kann daher den Zugriff der Vorstandsmitglieder auf Mitgliederdaten nicht mit einer fehlenden Verpflichtung auf das Datengeheimnis verweigern.

5.8.1.6
Versendung von E-Mails an Mitglieder im offenen Verteiler

Zwei Mitglieder einer politischen Partei beschwerten sich unabhängig voneinander, dass ihre jeweiligen Kreisverbände Informationen an die Parteimitglieder per E-Mail im offenen „An“ bzw. „Cc“ versenden und damit jeder E-Mail-Empfänger nachvollziehen kann, wer Mitglied der Partei ist. Die Parteimitglieder baten mich, ohne Nennung ihrer Namen einzuschreiten.

Ich habe in diesem Fall die betroffenen Kreisvorstände und auch den Landesvorstand über die Rechtslage informiert und mitgeteilt, dass das Aufführen der E-Mail-Adressen aller Empfänger in den offen lesbaren Feldern „An“ oder „Cc“ dazu führt, dass alle diese E-Mail-Adressen allen Empfängern bekannt gegeben werden. Aus datenschutzrechtlicher Sicht handelt es sich dabei in jedem Einzelfall um die Übermittlung personenbezogener Daten, die nicht erforderlich war, die ohne Rechtsgrundlage erfolgte und damit datenschutzrechtlich unzulässig war.

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. Sie dürfen ansonsten **nur als Blindkopie („bcc“)** verschickt werden, bei der eine unzulässige Übermittlung personenbezogener Daten über ein E-Mail-Adressierfeld ausgeschlossen ist. Unabhängig von der datenschutzrechtlichen Unzulässigkeit solcher Übermittlungen werden durch diese Adressiervarianten 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. Hinzu kommt die Gefahr, dass andere E-Mail-Empfänger die erhaltenen E-Mail-Adressen für unverlangte Werbe-E-Mails nutzen können und die hohe Zahl der eingehenden E-Mails zur Funktionsunfähigkeit eines E-Mail-Accounts führen kann.

Gleichzeitig habe ich die betroffenen Kreisverbände und den Landesverband darauf hingewiesen, dass der E-Mail-Versand mit offenem Verteiler eine Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG darstellt (s. a. 42. Tätigkeitsbericht, Ziff. 4.1.3).

§ 43 Abs. 2 Nr. 1 BDSG

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

...

Die betroffenen Kreisverbände zeigten sich einsichtig und versicherten, dafür Sorge zu tragen, dass keine E-Mails mehr im offenen Verteiler versendet werden. Der Landesverband erklärte, er werde die übrigen Kreisverbände noch mal ausdrücklich auf die Problematik und die Rechtslage aufmerksam machen und in dieser Hinsicht sensibilisieren und um Beachtung bitten.

5.8.2
Minderjährigenschutz in Vereinen – zum Umgang mit erweiterten Führungszeugnissen

Vereine dürfen einschlägig vorbestrafte Personen nicht in ihrer Kinder- und Jugendarbeit beschäftigen. Mit der Einsichtnahme in das erweiterte Führungszeugnis eines Betroffenen soll dies sichergestellt werden. Je nach Status des Vereins in der Jugendarbeit sind bei der Verarbeitung der aus den Führungszeugnissen gewonnenen Erkenntnisse unterschiedliche datenschutzrechtliche Regelungen zu beachten.

Mehrere Eingaben im Berichtsjahr zeigten, dass bei Mitarbeitern von Vereinen, die Jugendarbeit leisten, Unsicherheiten bestehen, wie mit den sensiblen Daten aus einem erweiterten Führungszeugnis datenschutzrechtlich korrekt umzugehen ist. Die Rechtslage für die Vereine ist in der Tat nicht leicht überschaubar.

5.8.2.1
Vereine als Träger der freien Jugendhilfe

Für Vereine mit dem Status „Träger der freien Jugendhilfe“ gilt § 72a Abs. 5 SBG VIII.

§ 72a Abs. 5 SGB VIII

Träger der öffentlichen und freien Jugendhilfe dürfen von den nach den Absätzen 3 und 4 eingesehenen Daten nur den Umstand, dass Einsicht in ein Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information erheben, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist. Die Träger der öffentlichen und freien Jugendhilfe dürfen diese erho-

benen Daten nur speichern, verändern und nutzen, soweit dies zum Ausschluss der Personen von der Tätigkeit, die Anlass zu der Einsichtnahme in das Führungszeugnis gewesen ist, erforderlich ist. Die Daten sind vor dem Zugriff Unbefugter zu schützen. Sie sind unverzüglich zu löschen, wenn im Anschluss an die Einsichtnahme keine Tätigkeit nach Absatz 3 Satz 2 oder Absatz 4 Satz 2 wahrgenommen wird. Andernfalls sind die Daten spätestens drei Monate nach der Beendigung einer solchen Tätigkeit zu löschen.

Vereine sind Träger der freien Jugendhilfe, wenn sie als solche gemäß § 75 SGB VIII anerkannt sind. Ein „schnelles" Indiz dafür ist eine staatliche Förderung. In der Regel ist mit dem Träger der staatlichen Förderung eine Vereinbarung abgeschlossen, die den Ausschluss einschlägig vorbestrafter Personen von der Jugendarbeit sicherstellt, § 72a Abs. 2 und 4 SGB VIII.

§ 72a Abs. 2 und 4 SGB VIII

(2) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sicherstellen, dass diese keine Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, beschäftigen.

(4) Die Träger der öffentlichen Jugendhilfe sollen durch Vereinbarungen mit den Trägern der freien Jugendhilfe sowie mit Vereinen im Sinne des § 54 sicherstellen, dass unter deren Verantwortung keine neben- oder ehrenamtlich tätige Person, die wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist, in Wahrnehmung von Aufgaben der Kinder- und Jugendhilfe Kinder oder Jugendliche beaufsichtigt, betreut, erzieht oder ausbildet oder einen vergleichbaren Kontakt hat. Hierzu sollen die Träger der öffentlichen Jugendhilfe mit den Trägern der freien Jugendhilfe Vereinbarungen über die Tätigkeiten schließen, die von den in Satz 1 genannten Personen auf Grund von Art, Intensität und Dauer des Kontakts dieser Personen mit Kindern und Jugendlichen nur nach Einsichtnahme in das Führungszeugnis nach Absatz 1 Satz 2 wahrgenommen werden dürfen.

Mit der Vereinbarung geben die Vereine eine Selbstverpflichtung gegenüber dem öffentlichen Träger ab, erforderliche präventive Schutzmaßnahmen zu ergreifen. Zu diesen Maßnahmen zählt auch die Anforderung der Vorlage eines erweiterten Führungszeugnisses nach § 30a BZRG von Betroffenen, um festzustellen, ob eine einschlägige Vorstrafe für einen Tätigkeitsausschluss vorliegt. Betroffenen wird zu diesem Zweck vom Bundeszentralregister das Führungszeugnis erteilt, wenn ein entsprechendes Anforderungsschreiben des Vereins mit Bezug auf § 72a SGB VIII vorgelegt wird.

§ 30a BZRG

(1) Einer Person wird auf Antrag ein erweitertes Führungszeugnis erteilt,

1. *wenn die Erteilung in gesetzlichen Bestimmungen unter Bezugnahme auf diese Vorschrift vorgesehen ist oder*
2. *wenn dieses Führungszeugnis benötigt wird für*

a) die Prüfung der persönlichen Eignung nach § 72a des Achten Buches Sozialgesetzbuch – Kinder- und Jugendhilfe –,
b) eine sonstige berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder
c) eine Tätigkeit, die in einer Buchstabe b vergleichbaren Weise geeignet ist, Kontakt zu Minderjährigen aufzunehmen.

(2) Wer einen Antrag auf Erteilung eines erweiterten Führungszeugnisses stellt, hat eine schriftliche Aufforderung vorzulegen, in der die Person, die das erweiterte Führungszeugnis vom Antragsteller verlangt, bestätigt, dass die Voraussetzungen nach Absatz 1 vorliegen. Im Übrigen gilt § 30 entsprechend.

Allerdings darf die Vorlage eines Führungszeugnisses nicht regelmäßig von allen neben- oder ehrenamtlich tätigen Personen, die Kontakt mit Kindern und Jugendlichen haben, verlangt werden. Der Wortlaut des Gesetzes verlangt vielmehr eine Abwägung und Differenzierung auf Intensität und Dauer des Kontakts.

§ 72a Abs. 5 SGB VIII regelt sodann [– allerdings dem Wortlaut nach für neben- oder ehrenamtlich tätige Personen (Fälle des § 72a Abs. 4 SGB VIII) –], wie datenschutzrechtlich mit den Erkenntnissen aus den Führungszeugnissen umzugehen ist:

- Das Führungszeugnis wird nur zur Einsicht vorgelegt, folglich darf es weder im Original noch in Kopie zu den Akten genommen werden.
- Es darf nur der Umstand, dass Einsicht genommen wurde, das Datum des Führungszeugnisses und die Information, ob eine einschlägige Verurteilung vorliegt, erhoben werden.
- Gespeichert, verändert oder genutzt werden dürfen die Daten nur, soweit dies zum Ausschluss des Tätigwerdens der betroffenen Person erforderlich ist.
- Eine Übermittlung der Daten ist nicht zulässig.
- Kommt es wegen eines Eintrages zur Ablehnung der Person, sind die Daten sofort zu löschen.
- Wird die Person tätig, dürfen Datum der Einsichtnahme und Datum des Führungszeugnisses für die Dauer der Beschäftigung gespeichert werden.
- Die Speicherung der Tatsache, dass keine einschlägige Vorstrafe vorlag, ist dagegen nicht erforderlich (sonst hätte es nicht zu einer Beschäftigung kommen dürfen).
- Wenn Daten gespeichert werden, sind diese drei Monate nach Beendigung der Tätigkeit zu löschen und bis dahin vor dem Zugriff Dritter zu schützen.

Bei Beschäftigten, die bei einem Verein, der freier Träger der Jugendhilfe ist, in einem arbeitsvertraglich geregelten, abhängigen, entgeltlichen und weisungsgebundenen Dienstverhältnis stehen, sieht § 72a SGB VIII keine Regelung für die weitere Verarbeitung der Daten aus dem Führungszeugnis vor. Es ist davon auszugehen, dass es der Gesetzgeber bei den allgemeinen Vorschriften zum Beschäftigtendatenschutz § 32 BDSG belassen wollte. Hieraus ergibt sich aber nichts wesentlich anderes als § 72a Abs. 5 SGB VIII regelt.

Für Beschäftigte gilt zunächst § 72a Abs. 1 Satz 1 SGB VIII als Datenerhebungsnorm. Danach ist das Führungszeugnis (nur) vorzulegen. Es wird weder die Aushändigung noch die Aufbewahrung beim Arbeitgeber verlangt. Eine Speicherung des Originals oder seine Kopie ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich (§ 32 BDSG) und damit datenschutzrechtlich unzulässig. Im Übrigen sind keine Gründe ersichtlich, warum bei Beschäftigten mehr Daten aus einem Führungszeugnis verarbeitet werden sollten als bei neben- oder ehrenamtlich Tätigen, wie oben dargestellt. Dies gilt insbesondere dann, wenn die persönliche Zuverlässigkeit der Betroffenen in regelmäßigen Abständen (ca. drei bis fünf Jahre) durch erneute Vorlage eines Führungszeugnisses überprüft und aktuell gehalten werden soll.

Zudem ist aus der Begründung des Gesetzentwurfes, mit dem die Regelung in das SGB VIII aufgenommen wurde, zu entnehmen, dass der Gesetzgeber für ehrenamtliche und hauptamtlich Tätige vergleichbare Regelungen zum Schutze der Kinder schaffen wollte (BTDrucks. 201/11, S. 46).

5.8.2.2
Sonstige Vereine (außerhalb der staatlichen Jugendhilfe)

Für Vereine, die nicht in die staatliche Jugendhilfe integriert sind, sich aber gleichwohl in der Kinder- und Jugendarbeit engagieren, gelten für die Erhebung, Verarbeitung und Nutzung der Daten aus dem erweiterten Führungszeugnis die allgemeinen Vorschriften des BDSG. Insbesondere sind §§ 28, 35 BDSG anwendbar, wenn neben- oder ehrenamtlich Tätige betroffen sind, da die Daten mittelbar aus der automatisierten Datenverarbeitung des Bundeszentralregisters stammen. §§ 32, 35 BDSG sind anwendbar, wenn es um Beschäftigtenverhältnisse geht, da die Vorschrift auch gilt, wenn die Datenverarbeitung nicht automatisiert erfolgt.

Ob ein Verein die Vorlage eines erweiterten Führungszeugnisses bei der Einstellung eines Beschäftigten oder bei der Beschäftigung eines neben- oder ehrenamtlich Tätigen verlangen kann, kann sich aus seiner Satzung, einer

evtl. Selbstverpflichtung zum Kinder- und Jugendschutz und dem Gefährdungspotenzial der zu verrichtenden Tätigkeiten mit den Minderjährigen ergeben. Auch in diesem Fall muss die Aufforderung zur Vorlage eines erweiterten Führungszeugnisses an den Betroffenen diesen Zweck bestätigen, damit vom Bundeszentralregister das Führungszeugnis erteilt wird, § 30a BZRG.

Wird ein erweitertes Führungszeugnis vorgelegt, dürfen im weiteren Verfahren auch nur die Daten erhoben, verarbeitet und gespeichert werden, die zur Zweckerfüllung der Tätigkeit bzw. zur Eingehung und Durchführung des Beschäftigungsverhältnisses bzw. der ehrenamtlichen Tätigkeit erforderlich sind. Dabei sollte die oben unter Ziff. 5.8.2.1 dargelegte spezialgesetzliche Wertung des Gesetzgebers in § 72a Abs. 5 SGB VIII Anhaltspunkte für die Beurteilung der Erforderlichkeit und der Relevanz der Nutzung der Daten im Hinblick auf die angestrebte konkrete Tätigkeit sein.

Unabhängig davon müssen alle Vereine intern regeln, welche (zuverlässige und geeignete) Person mit der Wahrnehmung der Einsichtnahme-Prozedur beauftragt wird und wie die Speicher- und Löschungsvorgaben eingehalten werden.

6. Bilanz

6.1
Prüfung der Hessischen Zentrale für Datenverarbeitung Hünfeld (42. Tätigkeitsbericht, Ziff. 3.3.2.2)

In diesem Jahr hatte sich die Hessische Zentrale für Datenverarbeitung (HZD) bemüht, die von mir aufgezeigten Mängel zu beseitigen. Dabei hat man sich in zwei Fällen entschieden, gleich auf eine neue Technik zu setzen, statt das bestehende System anzupassen. Auf meine vier wesentlichen Feststellungen hat die HZD wie folgt reagiert.

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

  Hier hat die HZD zeitnah eine Beschreibung erstellt und die Mittel zur Verfügung gestellt, dass solche Vorfälle doch erkannt werden können.

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

  Die HZD hat die Zahl der Personen mit Administratorrechten verringert, aber sie hat die mir genannte Zielgröße noch nicht erreicht.

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

  Die entsprechende Kontrollsoftware wurde 2014 eingerichtet und getestet. Sie soll in Kürze für einige Bereiche der Plattform zur Verfügung stehen. Sie muss dann noch auf die Justiz ausgedehnt werden.

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

  Hier hat sich die HZD entschieden, ein neues Ticketsystem einzuführen. Bei dem neuen Ticketsystem werden meine Anforderungen berücksichtigt.

7. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

7.1
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Beschäftigtendatenschutzgesetz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutz-Grundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutz-Grundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutz-Grundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen. Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater

Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielsweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

7.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wiederherzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wiederhergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

7.2.1
Anlage zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten

   Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptografische Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und er-

schweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich.

Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur

   Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.

   Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung

   Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.

   Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten

   Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security)/SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nicht-öffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten

   Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation

   Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen

   Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggfs. die Wahr-

scheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird.

Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internets oder Versuchen, Teile davon abzuschotten – dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen. Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können. Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

- alle Übertragungswege – sowohl vom Gerät zur Basisstation als auch innerhalb des Netzwerks des TK-Anbieters – verschlüsselt werden,
- für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,
- eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
- die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken.

Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen.

Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

   Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.

   Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

    Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.

    Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik

    Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

    Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

7.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Zur Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon, ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.
2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.
3. Die federführende Behörde und die zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.
4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.
5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurateziehung mit den Aufsichtsbehörden geklärt werden.
6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und

zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

7.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke – Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies – ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen – nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131a Abs. 3, § 131b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken, in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.
- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.
- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.
- Es ist sicherzustellen, dass
  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,
  - die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
  - die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

7.5
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014

Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa des Abstands von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotenzial immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internetdienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchstmöglicher Weise berücksichtigen:

– Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biome-

trischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4a BDSG rechtmäßig erfolgen.

– Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.
– Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
– Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
– Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.
– Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.

7.6
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. April 2014

Ende der Vorratsdatenspeicherung in Europa!

Der Europäische Gerichtshof hat in seinem Urteil vom 8. April 2014 die Europäische Richtlinie zur Vorratsspeicherung von Telekommunikations-Verkehrsdaten (Richtlinie 2006/24/EG) für ungültig erklärt. Dieses Urteil hat weitreichende Folgen für den Datenschutz in Europa.

Die Datenschutzbeauftragten des Bundes und der Länder haben die anlasslose und massenhafte Speicherung von Verkehrsdaten der Telekommunikation stets abgelehnt. Sie begrüßen die Entscheidung des Europäi-

schen Gerichtshofs als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses.

Der Europäische Gerichtshof hat in seinem Urteil der undifferenzierten und automatischen Totalerfassung solcher Daten eine klare Absage erteilt. Er hat darauf hingewiesen, dass schon die Pflicht zur anlasslosen Speicherung einen besonders schwerwiegenden Eingriff großen Ausmaßes in das Recht auf Privatleben und den Datenschutz der Betroffenen darstellt. Diese in der Europäischen Grundrechtecharta verbrieften Rechte dürften nur eingeschränkt werden, soweit dies absolut notwendig ist.

Die für ungültig erklärte Richtlinie entsprach diesen Vorgaben nicht, weil sie ohne jede Differenzierung, Einschränkung oder Ausnahme zur pauschalen Totalerfassung der Verkehrsdaten verpflichtete. Nach dem Urteil des Gerichtshofs kann eine undifferenzierte Pflicht zur anlasslosen und flächendeckenden Vorratsdatenspeicherung unionsrechtlich nicht mehr neu begründet werden. Die Absichtserklärung der Bundesregierung, zurzeit kein Gesetz zur Speicherung von Verkehrsdaten einzuführen, wird von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt. Etwaige Diskussionen auf europäischer Ebene sollten abgewartet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist ausdrücklich darauf hin, dass der Maßstab des EuGH auch für das anlasslose exzessive Überwachen durch sämtliche Nachrichtendienste gelten muss.

Zudem hält der Gerichtshof die Pflicht zur großflächigen Speicherung von personenbezogenen Daten nur dann für zulässig, wenn die Daten in der Europäischen Union gespeichert werden und damit unter die Kontrolle unabhängiger Datenschutzbehörden fallen. Dies zwingt auch zu einer Neubewertung z. B. der Fluggastdaten-Übermittlung in die USA und des Safe Harbor-Abkommens.

7.7
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014

Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen,

sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und der hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht,

muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen." In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

7.8
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014

Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BRDrucks. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Innern eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status' als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes- und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.
- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und Information im vorliegenden Entwurf des Bundesdatenschutzgesetzes nicht der Fall.
- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weitere Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

7.9
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014

Datenschutz im Kraftfahrzeug – Automobilindustrie ist gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen – etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehören:

– Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.
– Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.
– Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.
– Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Än-

derungen sind rechtzeitig anzuzeigen. Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

– Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
– Schließlich müssen durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

7.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014

Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double-Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA als auch in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Übernahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internetunternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordern nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 – Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutz-Grundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutz-Grundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist darauf hin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

7.11
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. Oktober 2014

Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 – C-131/12 – „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit frü-

heren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden. Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll – nach einer erfolgreichen Beschwerde des Betroffenen – der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internets muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.
- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.
- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

7.12
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln. Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensi-

bel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen. Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

7.12.1
Anlage zur Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, das dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291a, 291b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalogs im Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich, wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden. Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich. Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau (Szenarien 1N–4N).
2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemiologischen Krebsregistrierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. *Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.* Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedes für den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 4./5. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der An-

bindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

Ferner sind hohe (Szenarien 1–2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend (Szenarien 1W, 2W, 4W).

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse. Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wären Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI-TR 03116-1 entnommen sein (Szenarien 1–4).
5. Für die Identifizierung der Teilnehmer des Verfahrens, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rükkruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI-TR 03107-1 zu erfüllen (Szenarien 1–4).
6. *(optional)* Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291b SGB V verwendet werden, sobald diese verfügbar sind (Szenarien 1–4).
7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen (Szenarien 1–4).

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsselung einzusetzen (Szenarien 1–4).
9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann (Szenario 1).
10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen (Szenarien 2–4).
11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich (Szenarien 1–4).
12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein (Szenarien 1W–4W).
13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen (Szenarien 2+4).
14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet (Szenarien 2W+4W).
15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291a Abs. 5c SGB V bestimmt wurden (Szenarien 2–4).
16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt (Szenario 2).
17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind (Szenario 3).
18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Beste-

hen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen, muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können (Szenario 4).

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19. Ambulante Leistungserbringer müssen die „Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen (Szenarien 1–4).
20. Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind (Szenarien 1–4).
21. Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräten dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden (Szenarien 1–4).
22. Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders hohen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein (Szenarien 1–4).
23. Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss *(defense in depth)* (Szenarien 1W–4W).
24. Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschrän-

kung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs (Szenarien 1W–4W).

25. Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedarf besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig (Szenarien 1W–4W).
26. Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden (Szenario 4W).

Maßnahmen zur Gewährleistung der Authentizität der Daten

27. Da die übermittelten Daten einer folgenden Behandlung zugrundegelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind (Szenarien 1+4).
28. Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren (Szenarien 1+4).

Maßnahmen zur Transparenz und Datenschutzkontrolle

29. Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden (Szenarien 2–4).
30. Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten (Szenarien 2–4).
31. Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften (Szenario 4).

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

7.13
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014

Keine Pkw-Maut auf Kosten des Datenschutzes!

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen – beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten – mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-) elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte – bis zu 13 Monaten währende – Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weisen sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die Datenschutzbeauftragten des Bundes und der Länder mahnen die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

7.14
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen – zum Teil mehrfach wöchentlich –, von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKVVersorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“, gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

8. Beschlüsse des Düsseldorfer Kreises

8.1
Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 27. Januar 2014

Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird – ohne Anspruch auf Vollständigkeit – dargestellt, was zulässig ist.

8.1.1
Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 27. Januar 2014

Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Einleitung

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. An der Beantwortung der Fragen muss der Vermieter ein berechtigtes Interesse haben oder es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss das Recht des Mietinteressenten auf informationelle Selbstbestimmung Beachtung finden.

Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft ist nicht als das richtige Mittel zur Datenerhebung anzusehen. Eine wirksame Einwilligung erfordert nach § 4a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Dem Mietinteressenten wird dabei suggeriert, er habe bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht. Wird der Abschluss des Mietver-

trags von der Erhebung bestimmter Angaben beim Mietinteressenten abhängig gemacht, fehlt diese Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommt.

Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden: (a) dem Besichtigungstermin, (b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und (c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Die Zulässigkeit der Erhebung einer Selbstauskunft richtet sich im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht dann ein vorvertragliches Schuldverhältnis zum künftigen Vermieter, so dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Steht dem Vermieter für die Datenerhebung eine gesetzliche Grundlage nach § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG zur Verfügung, so kommt es auf die Anforderungen nach § 4a Abs. 1 Satz 1 BDSG nicht an bzw. ein Rückgriff auf das Konstrukt der Einwilligung wäre auch falsch, denn für den Mietinteressenten würde wiederum der Eindruck entstehen, dass die Offenbarung der Informationen seinem Wahlrecht unterliegt. Bei der Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG kommt es dann im Rahmen der Erforderlichkeitsprüfung darauf an, ob von Seiten des Interessenten aus Offenbarungspflichten bestehen bzw. ob von Vermieterseite aus zulässige Fragen gestellt werden. Unzulässige Fragen müssen demnach nicht beantwortet werden (Blank, in: Schmidt-Futterer, Kommentar zum Mietrecht, 11. Auflage 2013, § 543, Rn. 204). Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen des Mietinteressenten am Ausschluss der Datenerhebung bestehen.

Die folgende Darstellung ist nicht im Sinne einer abschließenden Aufzählung zu verstehen:

a) Besichtigungstermin

Strebt der Mietinteressent nur eine Besichtigung der Räumlichkeiten an, so wäre es etwa nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen.

Erfragt werden dürfen:

aa) Angaben zur Identifikation

Hierzu zählen Name, Vorname und Anschrift. Der Vermieter wäre auch befugt, im Falle der Besichtigung allein durch den Mietinteressenten die An-

gaben durch Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.

bb) Angaben aus Wohnberechtigungsschein

Der künftige Vermieter darf nach § 27 Abs. 1 Wohnraumförderungsgesetz (WoFG) eine Wohnung, die im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde, nur einem Wohnungssuchenden zum Gebrauch überlassen, wenn dieser ihm vorher seine Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweist. Möchte der Mietinteressent eine solche Wohnung besichtigen, sind Angaben zum Vorliegen eines Wohnberechtigungsscheins sowie zur genehmigten Wohnfläche und Anzahl der Wohnräume erforderlich, da nur in diesem Fall ein Besichtigungstermin sinnvoll ist. Eine Kopie des Wohnberechtigungsscheins darf erst nach der Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen, erfolgen, da die in dem Formular aufgeführten Angaben zu den Namen und Vornamen der im Haushalt des Mietinteressenten befindlichen Personen im Besichtigungstermin nicht erforderlich sind.

cc) Angaben zu Haustieren

Fragen des Vermieters nach dem beabsichtigten Einbringen von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Entsprechende Fragen sind zulässig, soweit dies nicht Kleintiere betrifft (z. B. Zierfische, Mäuse, Hamster).

b) Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen

aa) Familienstand und Angaben zu den im Haushalt lebenden Personen

Angaben zum Familienstand des Mietinteressenten werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein aus dieser Zwecksetzung heraus ist kein berechtigtes Vermieterinteresse gegeben, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen. Soweit nur ein Ehegatte den Wohn-Mietvertrag unterzeichnen möchte und im Hinblick auf die äußere Gestaltung des Mietvertrags und die mündlichen Absprachen nicht davon ausgegangen werden kann, dass auch der andere Ehegatte Mietvertragspartei wird, greift keine gesamtschuldnerische Haftung ein. Schließlich ginge auch das Argument ins Leere, von Vermieterseite aus einer möglichen Gebrauchsüberlassung an Dritte zuvorzukommen, denn nach § 553 Abs. 1 BGB hätte der Mieter im Regel-

fall ein berechtigtes Interesse daran, dem Ehegatten den Wohnraum zur Nutzung zu überlassen.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben dürfen zu diesen Personen nicht eingeholt werden, es sei denn, diese möchten Mietvertragspartner sein.

bb) Eröffnetes Insolvenzverfahren, Angabe einer Vermögensauskunft, Räumungstitel wegen Mietzinsrückständen

Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen (LG Bonn, Beschluss v. 16.11.2005, Az. 6 T 312/05 und 6 S 226/05).

Bei der Angabe einer Vermögensauskunft (§ 802c Abs. 3 ZPO) sind Mietzinsansprüche des Vermieters nicht in gleicher Weise gefährdet (LG Bonn, Beschluss v. 16.11.2005, Az. 6 T 312/05 und 6 S 226/05). Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften besteht, hängt u. a. davon ab, nach welchem Zeitraum gefragt wird. Ferner ist zu berücksichtigen, dass gemäß § 882f Satz 1 Nr. 4 ZPO eine Einsicht in das Schuldnerverzeichnis unter bestimmten Voraussetzungen möglich ist und zum Inhalt eines solchen Verzeichnisses auch Eintragungsanordnungen nach § 882c ZPO zählen. Nach § 882f Satz 1 Nr. 4 ZPO ist die Einsicht in das Schuldnerverzeichnis jedem gestattet, der darlegt, Angaben nach § 882b ZPO zu benötigen, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Im Hinblick auf den erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung des Mietinteressenten ist bei der Anwendung von § 882f Satz 1 Nr. 4 ZPO vor allem der Verhältnismäßigkeitsgrundsatz zu beachten. Ferner muss den wirtschaftlichen Nachteilen bedeutsames Gewicht zukommen (Utermark, in: Vorwerk/Wolf, Beck`scher Online-Kommentar ZPO, 2013, § 882f, Rn. 7). An die Zulässigkeit einer Datenerhebung beim Vollstreckungsgericht nach § 882f Satz 1 Nr. 4 ZPO sind ähnlich hohe Anforderungen zu stellen, wie im Rahmen einer Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG beim Mietinteressenten.

Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall

sein, wenn bezüglich eines bestehenden Wohnraummietverhältnisses mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht (AG Wolfsburg, Urteil v. 09.08.2000, Az. 22 C 498/99). Fragen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchgeführt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, werden als zulässig angesehen (LG Wuppertal, Urteil v. 17.11.1998, Az.: 16 S 149/98).

cc) Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit

Nach § 19 Abs. 1 und 3 AGG ist bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum eine unterschiedliche Behandlung im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zulässig. Es fehlt regelmäßig an der Erforderlichkeit der Datenerhebung, da die Anforderungen nach den §§ 19, 20 AGG kaum erfüllt sein werden. Hierfür müsste zur Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zunächst ein tragfähiges Vermietungskonzept vorliegen. Das Konzept muss auch zur Prüfung sachlicher Gründe (vgl. etwa § 20 Abs. 1 Nr. 4 AGG) Auskunft geben, die eine Ungleichbehandlung rechtfertigen und folglich zur Entschärfung von Konflikten beitragen können. Eine pauschale Abfrage der Angaben ist daher unzulässig.

dd) Vorstrafen und strafrechtliche Ermittlungsverfahren

Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Berücksichtigt werden muss zum einen, dass bestimmte Strafen nicht in ein polizeiliches Führungszeugnis aufzunehmen sind, § 32 Abs. 2 BZRG, und sich schon deshalb keine darüber hinausgehenden Mitteilungspflichten gegenüber einem Vermieter ergeben können. Weiterhin hat die Rechtsprechung eine Offenbarung von Vorstrafen bisher nur im Zusammenhang mit der Begründung von Arbeitsverhältnissen als zulässig angesehen, wenn ein klarer Bezug zu einer entsprechenden Tätigkeit besteht, wie etwa das Fragen nach Vermögensdelikten bei einer Beschäftigung im Kassenbereich eines Kreditinstituts. Dabei steht die Frage nach der Geeignetheit eines Bewerbers im Mittelpunkt. Bei der Anbahnung von Mietverhältnissen besteht grundsätzlich keine vergleichbare Gefährdungslage, da hier die Frage nach der Bonität des Mietinteressenten von zentraler Bedeutung ist. Gegen die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren spricht schon die verfassungsrechtlich und auch in Art. 6 Abs. 2 EMRK verankerte Unschuldsvermutung.

ee) Heiratsabsichten, Schwangerschaften, Kinderwünsche

Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und Kinderwünschen zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig. Eine Aufnahme von Kindern und Ehegatten in der Wohnung wäre für den Mietinteressenten schon nicht erlaubnispflichtig im Sinne von § 553 Abs. 1 Satz 1 BGB, denn diese Personen sind in Anwendung von Art. 6 Abs. 1 GG bereits keine Dritten (§ 553 Abs. 1 BGB), sondern nahe Familienangehörige. Der Mieter muss die Aufnahme von Familienangehörigen nur anzeigen. Einer Aufnahmeerlaubnis durch den Vermieter bedarf es nicht.

ff) Mitgliedschaften in Parteien und Mietvereinen

Es besteht keine Verpflichtung, über die Zugehörigkeit zu Parteien oder Mietervereinen Auskunft zu geben. Mit den Angaben wird zudem noch keine Aussage zur Bonität des Mietinteressenten bzw. zu dessen Zahlungsfähigkeit und Zahlungswilligkeit getroffen.

gg) Angaben zum Arbeitgeber, zum Beschäftigungsverhältnis und zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

hh) Einkommensverhältnisse

Die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens wäre jedoch auch die Angabe einer bestimmten Betragsgrenze durch den Mietinteressenten ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird. Im Hinblick auf die monatlichen Belastungen ist die Erfragung der Forderungsgründe (Unterhaltsverpflichtungen, Darlehensverbindlichkeiten etc.) unzulässig, da dies für die Beurteilung der Bonität nicht erforderlich ist.

Fragen nach den Einkommensverhältnissen sind unzulässig, wenn die Mietzahlungen vollständig von dritter Stelle für den Mieter übernommen und direkt an den Vermieter geleistet werden sollen, was bei Empfängern von Ar-

beitslosengeld II der Fall sein kann. Empfänger von Arbeitslosengeld II müssen für die Durchführung einer solchen Direktzahlung gegenüber dem Jobcenter eine entsprechende Erklärung abgeben, § 22 Abs. 7 Satz 1 SGB II. Direktzahlungen an den Vermieter werden nach § 22 Abs. 7 Satz 2 SGB II von Amts wegen vorgenommen, wenn eine zweckentsprechende Verwendung der gewährten Mittel durch den Empfänger von Arbeitslosengeld II nicht sichergestellt ist.

ii) Angaben zu bisherigen Vermietern

Fragen nach den Kontaktinformationen aktueller oder früherer Vermieter des Mietinteressenten (z. B. Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig. Solche Angaben wären für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich und würden eine dem Grundsatz der Direkterhebung (§ 4 Abs. 2 Satz 1 BDSG) widersprechende Datenerhebung bei Dritten über den Mietinteressenten ermöglichen.

c) Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten

Der künftige Vermieter möchte nun mit dem einzigen Mietinteressenten für eine konkrete Wohnung einen Mietvertrag schließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.

aa) Nachweise zu den Einkommensverhältnissen

Der künftige Vermieter kann bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen darauf hinweisen, dass für den Fall einer positiven Entscheidung für den Mietinteressenten quasi unmittelbar vor Unterzeichnung des Vertrags noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z. B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie – jeweils unter Schwärzung der nicht erforderlichen Angaben. Als Nachweis ist auch eine Bescheinigung des Arbeitgebers ausreichend, dass die Angaben des Mietinteressenten bezüglich der Angabe einer bestimmten Nettobetragsgrenze, die überschritten wird, zutreffend sind.

bb) Vorlage der Selbstauskunft nach Anfrage bei einer Auskunftei

Der künftige Vermieter benötigt Informationen zu den wirtschaftlichen Verhältnissen des Mietinteressenten, um dessen Zahlungsfähigkeit bezüglich

des Mietzinses beurteilen zu können. Selbstauskünfte, die Mietinteressenten bei Auskunfteien (z. B. SCHUFA) selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse als für eine solche Beurteilung erforderlich sind. Schon aus diesem Grund wäre die Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig.

Da die Verwendung von Einwilligungserklärungen gegenüber dem Mietinteressenten in Formularen zur Selbstauskunft nicht als das richtige Mittel zur Datenerhebung anzusehen ist, wäre auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, nicht rechtmäßig. Zur Einholung von Bonitätsauskünften über den Mietinteressenten wäre der Vermieter nur dann befugt, wenn die Voraussetzungen einer gesetzlichen Vorschrift (§ 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG) erfüllt sind. Vgl. zur Einholung von Bonitätsauskünften über Mietinteressenten gegenüber Auskunfteien den Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009 „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“.

8.2
Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 25./26. Februar 2014

Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbrauchern in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in **eigener** Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

8.3
Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 25./26. Februar 2014

Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nicht-öffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras – jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt – datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öf-

fentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.

8.4
Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internetdienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internetdienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internetdienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden. Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der frei-

heitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:
   – Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   – Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.
   – Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
   – Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
3. Beachtung des Prinzips „privacy by default“:
   Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung

bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

Sachwortverzeichnis zum 43. Tätigkeitsbericht