18. Wahlperiode

Drucksache **18/5409**

HESSISCHER LANDTAG

20. 03. 2012

Vierzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2011
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes vom 7. Januar 1999

Eingegangen am 20. März 2012 · Ausgegeben am 26. März 2012
Druck und Auslieferung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 40. Tätigkeitsbericht

AAL	engl.: Ambient Assisted Living (altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben)
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
AKKStelleG	Akkreditierungsstellengesetz
AKLS	Automatisches Kennzeichenlesesystem
Art.	Artikel
AufenthG	Aufenthaltsgesetz
Az.	Aktenzeichen
AZR	Ausländerzentralregister
BauGB	Baugesetzbuch
BDSG	Bundesdatenschutzgesetz
BDSG-E	(Änderungs-)Entwurf zum Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BIBO	Be-In/Be-Out
BIOS	Basic Input Output System
BITKOM	Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BNetzA	Bundesnetzagentur
BPolG	Bundespolizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BTDrucks.	Bundestagsdrucksache
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	zirka
CC	Common Criteria
CD	Compact Disc

CDU	Christlich Demokratische Union Deutschlands
CICO	Check-In/Check-Out
DIN	Deutsches Institut für Normung
DLR	Deutsches Zentrum für Luft- und Raumfahrt e.V.
DNA	engl.: Deoxyribonucleic acid (Desoxyribonukleinsäure)
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DuD	Zeitschrift Datenschutz und Datensicherheit
DVD	Digital Versatile Disc
eANV	elektronisches Abfallnachweisverfahren
EAÜ	elektronische Aufenthaltsüberwachung
EAW	engl.: European Arrest Warrant (europäischer Haftbefehl)
EC	engl.: electronic cash
EFS	elektronischer Fahrschein
EGMR	Europäischer Gerichtshof für Menschenrechte
EKD	Evangelische Kirche in Deutschland
ELV	elektronisches Lastschriftverfahren
ENISA	European Network and Information Security Agency
ePR	elektronisches Personenstandsregister
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FAQs	engl.: Frequently Asked Questions (Informationen zu besonders häufig gestellten Fragen)
FAZ	Frankfurter Allgemeine Zeitung
FDP	Freie Demokratische Partei
ff.	fortfolgende/r/s
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GK	Gemeinsame Kontrollinstanz
GMBl	Gemeinsames Ministerialblatt
GPS	engl.: Global Positioning System (globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung)

GÜL	Gemeinsame Überwachungsstelle der Länder
GVBl.	Gesetz- und Verordnungsblatt für das Land Hessen
GWZ	Gebäude- und Wohnungszählung
HARIS	Hessisches Analyse- und Recherchesystem
HBG	Hessisches Beamtengesetz
HBS	Hessische Bezügestelle
HDE	Handelsverband Deutschland – Der Einzelhandel
HDSG	Hessisches Datenschutzgesetz
HessLStatG	Hessisches Landesstatistikgesetz
HGO	Hessische Gemeindeordnung
HKHG	Hessisches Krankenhausgesetz
HKO	Hessische Landkreisordnung
HLfV	Hessisches Landesamt für Verfassungsschutz
HLKA	Hessisches Landeskriminalamt
HMDIS	Hessisches Ministerium des Innern und für Sport
HMG	Hessisches Meldegesetz
HSchG	Hessisches Schulgesetz
HSL	Hessisches Statistisches Landesamt
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HSÜG	Hessisches Sicherheitsüberprüfungsgesetz
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HWBG	Hessisches Weiterbildungsgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. F.	in der Fassung
IaaS	Infrastructure as a Service
ICANN	Internet Corporation for Assigned Names and Numbers
ID-Nummer	Identifikationsnummer
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
IP	Internet Protocol
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization (Internationale Organisation für Normung)
IT	Informationstechnik
JAG	Juristenausbildungsgesetz

Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
KUNO	Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
LAN	engl.: Local Area Network (lokales Netzwerk)
LRM	Landesreferenzmodell
LTDrucks.	Landtagsdrucksache
NADIS	Nachrichtendienstliches Informationssystem
NADIS WN	Nachrichtendienstliches Informationssystem als Wissensnetz
NJW	Neue Juristische Wochenschrift
NORAH	Noise Related Annoyance, Cognition, and Health (Lärmwirkungsstudie)
Nr.	Nummer
o. Ä.	oder Ähnliche/r/s
o. g.	oben genannte/r/s
OFD	Oberfinanzdirektion
OH	Orientierungshilfe
ÖPNV	Öffentlicher Personennahverkehr
PaaS	Platform as a Service
PC	Personalcomputer
PDCA	Plan-Do-Check-Act
PIN	engl.: Personal Identification Number (persönliche Geheimzahl)
POLAS	Polizeiauskunftssystem
Rdnr.	Randnummer
RFID	Radio Frequency Identification
RMV	Rhein-Main-Verkehrsverbund
S.	Seite
s.	siehe
SaaS	Software as a Service
SDÜ	Schengener Durchführungsübereinkommen

SEPA	engl.: Single European Payment Area (Initiative zur Etablierung eines einheitlichen Euro-Zahlungsverkehrsraumes)
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SIS II	Schengener Informationssystem der zweiten Generation
SLA	Service Level Agreement
sog.	sogenannte
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SUZ	Sozialwissenschaftliches Umfragezentrum GmbH
SWIFT	Society for Worldwide Interbank Financial Telecommunication (Internationale Genossenschaft der Geldinstitute)
TFTP	Terrorist Finance Tracking Program (US-System zur Aufspürung von Terrorismus-finanzierungen)
TFTS	Terrorist Finance Tracking System (Europäisches System zur Aufspürung von Terrorismusfinanzierung)
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
ThürDSG	Thüringer Datenschutzgesetz
u. U.	unter Umständen
UAG	Unterarbeitsgruppe
UNH	Gemeinnützige Umwelthaus GmbH
USA	United States of America (Vereinigte Staaten von Amerika)
USB	Universal Serial Bus
VDV	Verband Deutscher Verkehrsunternehmen
VerfSchutzG	Verfassungsschutzgesetz
vgl.	vergleiche
VIP	engl.: very important person (prominente Persönlichkeit)

WN	Wissensnetz
z. B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter
ZensG	Zensusgesetz
Ziff.	Ziffer
ZRP	Zeitschrift für Rechtspolitik

Register der Rechtsvorschriften

AKKStelleG	Gesetz über die Akkreditierungsstelle (Akkreditierungsstellengesetz – AKKStelleG) vom 31. Juli 2009 (BGBl. I S. 2625), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 3044)
Allgemeine Verwaltungsvorschrift (AVwV) zum Gesetz über das Ausländerzentralregister und zur Verordnung zur Durchführung des Gesetzes über das Ausländerzentralregister	vom 26. Okt. 2009 (GMBl, S. 1293)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) i. d. F. vom 25. Feb. 2008 (BGBl. I S. 162), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 3044)
BauGB	Baugesetzbuch i. d. F. vom 23. Sept. 2004 (BGBl. I S. 2414), zuletzt geändert durch Gesetz vom 22. Juli 2011 (BGBl. I S. 1509)
BDSG	Bundesdatenschutzgesetz i. d. F. vom 14. Jan. 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14. Aug. 2009 (BGBl. I S. 2814)
BDSG-E	(Änderungs-)Entwurf zum Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch i. d. F. vom 2. Jan. 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Gesetz vom 27. Juli 2011 (BGBl. I S. 1600)
BPolG	Gesetz über die Bundespolizei (Bundespolizeigesetz) vom 19. Okt. 1994 (BGBl. I S. 2978), zuletzt geändert durch Gesetz vom 31. Juli 2009 (BGBl. I. S. 2507)
BSI-Gesetz	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. Aug. 2009 (BGBl. I S. 2821)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG) i. d. F. vom 21. Sept. 1984, zuletzt geändert durch Gesetz vom 14. Aug. 2009 (BGBl. I S. 2827)
EG-Richtlinie Datenschutzrichtlinie für elektronische Kommunikation	Richtlinie des Europäischen Parlaments und des Rates Nr. 2009/136 vom 25. Nov. 2009 (ABl. EG Nr. L 337/11) zur Änderung der EG-Richtlinie Nr. 2002/22 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der EG-Richtlinie Nr. 2002/58 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der EG-Verordnung Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz

EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	EG-Datenschutzrichtlinie Nr. 95/46 vom 24. Okt. 1995 (ABl. EG Nr. L 281/31), in nationales Recht umgesetzt durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl. I S. 904)
EUROPOL-Beschluss	Beschluss des Rates Nr. 2009/371 vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts (ABl. EU Nr. L 121/37)
GewO	Gewerbeordnung i. d. F. vom 22. Feb. 1999 (BGBl. I S. 202), zuletzt geändert durch Gesetz vom 29. Juli 2009 (BGBl. I S. 2258)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 21. Juli 2010 (BGBl. I S. 944)
HBG	Hessisches Beamtengesetz i. d. F. vom 11. Jan. 1989 (GVBl. I 1989 S. 26), zuletzt geändert durch Gesetz vom 25. Nov. 2010 (GVBl. I S. 410)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 7. Jan. 1999 (GVBl. I S. 98)
Hessisches Ausführungsgesetz zum Zensusgesetz 2011	vom 23. Juni 2010 (GVBl. I S. 178)
Hessisches Hochschulgesetz	vom 14. Dez. 2009, zuletzt geändert durch Gesetz vom 21. Dez. 2010 (GVBl. I S. 617, 618)
Hessisches Lehrerbildungsgesetz	i. d. F. vom 28. Sept. 2011 (GVBl. I S. 590)
HessLStatG	Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz) vom 19. Mai 1987 (GVBL. I S. 67), zuletzt geändert durch Gesetz vom 23. Juni 2010 (GVBl. I S. 178, 181)
HGO	Hessische Gemeindeordnung i. d. F. vom 7. März 2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 16. Dez. 2011 (GVBl. I S. 786)
HImVO	Verordnung über das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation, das Studium als Gasthörerin oder Gasthörer, das Teilzeitstudium und die Verarbeitung personenbezogener Daten der Studierenden an den Hochschulen des Landes Hessen vom 24. Feb. 2010 (GVBl. I S. 94)
HKO	Hessische Landkreisordnung i. d. F. vom 7. März 2005 (GVBl. I S. 183), zuletzt geändert durch Gesetz vom 16. Dez. 2011 (GVBl. I S. 786, 794)
HLbGDV	Verordnung zur Durchführung des Hessischen Lehrerbildungsgesetzes vom 28. Sept. 2011 (GVBl. I S. 615)

HMG	Hessisches Meldegesetz i. d. F. vom 10. März 2006 (GVBl. I S. 66), zuletzt geändert durch Gesetz vom 22. Nov. 2010 (GVBl. I S. 403, 404)
HSchG	Hessisches Schulgesetz i. d. F. vom 14. Juni 2005 (GVBl. I S. 442), zuletzt geändert durch Gesetz vom 16. Sept. 2011 (GVBl. I S. 420)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14. Jan. 2005 (GVBl. I. S. 14), zuletzt geändert durch Gesetz vom 14. Dez. 2009 (GVBl. I S. 635)
HSÜG	Hessisches Sicherheitsüberprüfungsgesetz vom 28. Sept. 2007 (GVBl. I S. 623)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15. Jan. 2010 (GVBl. I S. 18)
HWBG	Gesetz zur Förderung der Weiterbildung und des lebensbegleitenden Lernens im Lande Hessen (Hessisches Weiterbildungsgesetz) vom 25. Aug. 2001 (GVBl. I, S. 370), zuletzt geändert durch Gesetz vom 21. Nov. 2011 (GVBl. I S. 673)
ISO/IEC 27001	ISO/IEC 27001 “Information technology – Security techniques – Information Security Management Systems – Requirements”, First edition 2005-10-15 – Ref. Number ISO/IEC 27001:2005(E). Deutsche Übersetzung als DIN-Norm DIN ISO/IEC 27001: 2008
ISO/IEC 27006	ISO 27006 “Information technology – Security techniques. Requirements for bodies providing audit and certification of information security management systems”, First edition 2007-03-01 – Ref. Number ISO/IEC 27006: 2007. The revised version published in December 2011 will go through a systematic review process.
JAG	Gesetz über die juristische Ausbildung (Juristenausbildungsgesetz) i. d. F. vom 15. März 2004, zuletzt geändert durch Gesetz vom 24. Mai 2011 (GVBl. I S. 206)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im BGBl. Teil III, Gliederungsnummer 440-3 veröffentlichten bereinigten Fassung; zuletzt geändert durch Gesetz vom 16. Febr. 2001 (BGBl. I S. 266)
SDÜ	Schengener Durchführungsübereinkommen vom 14. Juni 1985 (BGBl. 1993 II S. 1010), zuletzt geändert durch Verordnung Nr. 265/2010 (ABl. EU Nr. L85 S. 1)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil i. d. F. vom 11. Dez. 1975 (BGBl I S. 3015), zuletzt geändert durch Gesetz vom 20. Dez. 2011 (BGBl. I S. 2854)

SGB II	Zweites Buch Sozialgesetzbuch – Grundsicherung für Arbeitsuchende i. d. F. vom 13. Mai 2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 3057
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung i. d. F. vom 20. Dez. 1988 (BGBl. I S. 2477), zuletzt geändert durch Gesetz vom 28. Juli 2011 (BGBl. I S. 1622)
SGB VIII	Achtes Buch Sozialgesetzbuch – Kinder- und Jugendhilfe i. d. F. vom 14. Dez. 2006 (BGBl. I S. 3134), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 2975)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz i. d. F. vom 18. Jan. 2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 2983)
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Gesetz vom 17. Juli 2009 (BGBl. I S. 2091)
StGB	Strafgesetzbuch i. d. F. vom 13. Nov. 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 6. Dez. 2011 (BGBl. I S. 2557)
StPO	Strafprozessordnung i. d. F. vom 7. Apr. 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 23. Juni 2011 (BGBl. I S. 1266)
StPO	Strafprozessordnung i. d. F. vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 22. Dez. 2011 (BGBl. I S. 3044)
SWIFT-Abkommen	Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP-Abkommen; ABl L195 vom 27. Juli 2010, S. 3)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 3 des Gesetzes vom 24. März 2011 (BGBl. I S. 506)
TMG	Telemediengesetz vom 26. Febr. 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692)
VerfSchutzG	Gesetz über das Landesamt für Verfassungsschutz vom 19. Dez. 1990 (GVBl. I S. 753), zuletzt geändert durch Gesetz vom 28. Sept. 2007 (GVBl. I S. 623, 633)

ZensG 2011	Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011) vom 8. Juli 2009 (BGBl. I S. 1781)

Kernpunkte

1. Der Berichtszeitraum dieses Tätigkeitsberichtes war wesentlich durch die Neuordnung des Datenschutzes in Hessen geprägt. Durch das vom Landtag einstimmig beschlossene Gesetz zur Neuordnung des Datenschutzes und zur Wahrung der Unabhängigkeit des Datenschutzbeauftragten vom 20. Mai 2010 (GVBl. I S. 208) wurde die Datenschutzkontrolle für den öffentlichen und nicht öffentlichen Bereich bei meiner Behörde vereint. Dies hat Auswirkungen auf meine Behörde, aber auch auf diesen erstmals beide Bereiche betreffenden Tätigkeitsbericht (Ziff. 1.1 und 1.2).

2. Im Umfeld des Frankfurter Flughafens soll eine Lärmwirkungsstudie zu den gesundheitlichen Auswirkungen des Flug- sowie Schienen- und Straßenlärms in den Jahren 2011 bis 2014 durchgeführt werden. Ziel der Studie ist es, eine möglichst repräsentative und wissenschaftlich abgesicherte Beschreibung der Auswirkungen des Lärms von Flug-, Schienen- und Straßenverkehr im Rhein-Main-Gebiet auf die Gesundheit und Lebensqualität der betroffenen Wohnbevölkerung zu erhalten. Hierzu soll eine Vielzahl von personenbezogenen Daten erhoben und ausgewertet werden. Ich habe das Konsortium, das die Studie durchführt, bei der Erstellung des detaillierten Datenschutzkonzeptes ausführlich beraten (Ziff. 3.7.1).

3. Die Volkszählung (Zensus) 2011 war eines der zentralen Themen im vergangenen Jahr und wurde von mir datenschutzrechtlich intensiv und mit hohem Aufwand begleitet. Bei den 33 Erhebungsstellen des Landes sowie im Zusammenhang mit der Einschaltung privater Unternehmen für den Versand der Erhebungsunterlagen und deren Aufbereitung gab es zwar kleinere Mängel, aber keine das Verfahren datenschutzrechtlich in Frage stellenden Unregelmäßigkeiten (Ziff. 3.7.2).

4. Auch in Hessen werden Projekte zum Einsatz intelligenter Assistenzsysteme für ein selbstbestimmtes Leben im Alter (AAL) entwickelt. Bestandteil derartiger Projekte ist stets die Verarbeitung sensitiver Gesundheitsdaten durch mehrere Projektbeteiligte. Angemessene Datenschutzkonzepte müssen in die Ausgestaltung der Projekte von Anfang an einbezogen werden (Ziff. 3.8.2).

5. Im Sozialbereich habe ich mich verschiedenen grundsätzlichen Fragestellungen gewidmet. Ein Thema war die Zusammenarbeit von SGB II-Stellen (Jobcenter) mit Jugendämtern und der Datenaustausch zwischen diesen Stellen. Die unterschiedlichen sozialdatenschutzrechtlichen Regelungen stehen einer Zusammenarbeit dieser Stellen nicht im

Wege (Ziff. 3.9.1). Zu weit gehen allerdings SGB II-Stellen, wenn sie ohne konkreten Anlass in sozialen Netzwerken zu ihrer Klientel recherchieren; eine solche Recherche ist nur im Einzelfall bei konkreten Anhaltspunkten zulässig (Ziff. 3.9.3).

6. Für Melderegisterauskünfte an Parteien und andere Träger von Wahlvorschlägen zu Wahlwerbezwecken sieht das Melderecht aus gutem Grund keine Übermittlung via E-Mail vor; sie können nur als Ausdrucke oder durch Übermittlung auf Datenträgern gewährt werden (Ziff. 4.3).

7. Auch in diesem Jahr haben Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Zusammenarbeit mit dem Düsseldorfer Kreis, dem Koordinierungsgremium der Aufsichtsbehörden für den nicht öffentlichen Bereich, Orientierungshilfen für die Praxis erarbeitet.

   – Die Orientierungshilfe Krankenhausinformationssysteme wurde erarbeitet, weil die Umsetzung der datenschutzrechtlichen Anforderungen an die Zugriffsausgestaltung von Krankenhausinformationssystemen immer wieder Probleme aufwirft. Die Orientierungshilfe wendet sich insbesondere an Krankenhausträger, Anwender und Hersteller einschlägiger Software sowie an interne Datenschutzbeauftragte und soll diesen eine detaillierte Orientierung ermöglichen (Ziff. 3.8.3 und http://www.datenschutz.hessen.de/ft-gesundheit.htm).

   – Die Orientierungshilfe Cloud Computing betrifft ein höchst aktuelles Thema und bereitet die datenschutzrelevanten Gesichtspunkte dieser Thematik auf, um eine erste Orientierung zu geben. Es wird erforderlich sein, diese Entwicklung auch künftig zeitnah zu begleiten (Ziff. 6.1 und 11.1; http://www.datenschutz.hessen.de/ft-oh_technik.htm).

8. Bei Zahlungen mit der EC-Karte im Wege des elektronischen Lastschriftverfahrens (ELV) – also dem Verfahren, das ohne Eingabe der PIN auskommt – ist für den Händler nicht sicher, ob die Forderung tatsächlich beglichen oder die Lastschrift zurückgewiesen wird. Aufgrund der immer wieder vorkommenden Forderungsausfälle beim ELV und zur Abwehr von missbräuchlichem Karteneinsatz (z. B. durch Diebe und Betrüger) wurden Verfahren zur Vermeidung und Reduzierung dieser Risiken entwickelt. Dabei sind auch die berechtigten (Datenschutz-) Interessen der Kunden zu beachten. Die Aufsichtsbehörden, die für die Kontrolle der meisten einschlägigen Unternehmen tätig sind, haben in einer Arbeitsgruppe Anforderungen und Abläufe analysiert und Empfehlungen für eine datenschutzgerechte Ausgestaltung des ELV gegeben (Ziff. 5.1).

1. Einführung

1.1
Allgemeines

Der Berichtszeitraum des 40. Tätigkeitsberichts stand ganz im Zeichen der Zusammenlegung von privatem und öffentlichem Bereich beim Datenschutz, die durch das Gesetz zur Neuordnung des Datenschutzes und zur Wahrung der Unabhängigkeit des Datenschutzbeauftragten in Hessen vom 20. Mai 2010 vollzogen wurde (GVBl. I S. 208), das zum 1. Juli 2011 in Kraft trat. Die Vorgeschichte dieses Gesetzes und die mit ihm verbundenen rechtlichen Probleme sind im 39. Tätigkeitsbericht für das Jahr 2010 behandelt. Die weitere Entwicklung ist unten unter Ziff. 1.2 skizziert. Es galt die vom EU-Recht geforderte Unabhängigkeit der Datenschutzkontrolle im öffentlichen und privaten Bereich mit deutschen verfassungsrechtlichen Strukturprinzipien in Einklang zu bringen. Nun kommt es darauf an, die mit der Zusammenlegung des öffentlichen und privaten Bereichs verknüpfte Hoffnung auf eine Verbesserung des Datenschutzes zu erfüllen. Dabei dürfen freilich nicht die grundlegenden strukturellen Unterschiede zwischen öffentlichem und privatem Bereich ignoriert werden. Die Kontrolle im öffentlichen Bereich ist zwar umfassend, betrifft aber das Verhältnis von Hoheitsträgern untereinander. Dem Hessischen Datenschutzbeauftragten stehen daher nur Beanstandungsrechte zu. Im privaten Bereich ist der Hessische Datenschutzbeauftragte dagegen zu außenwirksamen Maßnahmen befugt. Aber auch inhaltlich unterscheidet sich die Tätigkeit im öffentlichen Bereich grundlegend von der privaten Lebensgestaltung. Dies hängt mit der die kontinentaleuropäische Rechtsordnung prägenden Unterscheidung zwischen öffentlichem und privatem Recht zusammen.

Öffentlich-rechtliche Grundsätze stehen im Gegensatz zu privatrechtlichen Grundsätzen, wobei die auf das römische Recht zurückgehende Unterscheidung nie trennscharf geglückt ist. Kategorial lag Ulpian richtig, nach dem der Staat seine Interessen öffentlich-rechtlich verfolgt, während die Privaten abgesondert, eben privat ihre eigenen Interessen mit den Mitteln des Privatrechts zu verfolgen haben (Digesten 1.1.1). Die Unterscheidung ist für eine freiheitliche Rechtsordnung konstitutiv. Privatheit bedeutet Privatautonomie und grundsätzlich Freiheit vor staatlichem Zwang. Auch eine Grundrechtsbindung ist im Verhältnis Privater untereinander grundsätzlich ausgeschlossen. Dem steht das öffentliche Recht als Amtsrecht des Staates gegenüber, das die Befugnisse von Hoheitsträgern begründet und zugleich begrenzt. Das Grundrecht auf informationelle Selbstbestimmung und die sonstigen Datenschutzgrundrechte gelten hier unmittelbar. Im Verhältnis von Privaten untereinander muss die Geltung von Datenschutzgrundsätzen erst

angeordnet werden und die der Anordnung zugrunde liegende Güterabwägung ist auch bei der Durchsetzung im Wege der Datenschutzkontrolle zu berücksichtigen. Die Datenschutzkontrolle ist hier mit Eingriffen in Rechte verbunden und unterliegt dem Gesetzesvorbehalt und der Rechtschutzgarantie Betroffener. Eine klare Unterscheidung zwischen öffentlichem und privatem Recht und zwischen öffentlichem und privatem Bereich ist allerdings kaum noch möglich. Zum einen kann sich der Staat zur Erfüllung seiner Aufgaben Privater oder zur eigenen Betätigung der Regelungen des Privatrechts bedienen. Er bleibt dann aber an das Gemeinwohl gebunden. Öffentlich-rechtliche Bindungen bestehen direkt. Umgekehrt können Private zum Schutz anderer Privater Gemeinwohlbindungen unterworfen werden. Sie handeln dann jedoch immer noch im privaten Interesse. Gleichwohl erleidet das Privatrecht einen Qualitäts- und Bedeutungswandel, weil nunmehr das öffentliche Interesse in der Form von Regulierungen in das Privatrecht einfließt. Diese skizzierten Entwicklungen geben nur einen ersten Eindruck von den rechtlichen Schwierigkeiten, vor die sich der Datenschutz aus einer Hand gestellt sieht. Sie erklärt auch, weshalb der Gesetzgeber nicht alle Schwierigkeiten in einem ersten Anlauf bewältigen konnte.

1.2
Entwicklung des Datenschutzes in Hessen

1.2.1
Änderungen des Hessischen Datenschutzgesetzes

Nach der Entscheidung des EUGH vom 9. März 2010 – C-518/07 (NJW 2010, 1265) war auch die Organisation der Datenschutzkontrolle in Hessen europarechtswidrig, weil die Aufsichtbehörde für den Datenschutz im nicht öffentlichen Bereich in den Regierungsstrang eingegliedert und nicht – wie es die EG-Datenschutzrichtlinie in Art. 28 fordert – „völlig unabhängig“ installiert war.

Die Fraktionen der CDU, SPD, FDP und BÜNDNIS 90/DIE GRÜNEN hatten sich zum 40. Jahrestag des Inkrafttretens des ersten Hessischen Datenschutzgesetzes auf die Zusammenlegung der Datenschutzaufsicht in Hessen unter dem Dach des Hessischen Datenschutzbeauftragten und eine Stärkung der Unabhängigkeit verständigt („Wiesbadener Erklärung“ vom 7. Oktober 2010, 39. Tätigkeitsbericht Ziff. 1.1). Mit der Umsetzung der in der Wiesbadener Erklärung angekündigten Änderung des Datenschutzgesetzes und der Ausarbeitung eines Gesetzesentwurfs war eine interfraktionelle Arbeitsgruppe unter Beteiligung von Beschäftigten des Hessischen Innen-

ministeriums, des Regierungspräsidiums in Darmstadt und mir befasst. Nach Verhandlungen der Details ist der Gesetzentwurf als gemeinsamer Änderungsantrag zu dem von der SPD eingebrachten Gesetzentwurf (LTDrucks. 18/3869 zu LTDrucks. 18/375) ins Parlament eingebracht und dort am 20. Mai 2010 verabschiedet worden (Gesetz zur Neuordnung des Datenschutzes und Wahrung der Unabhängigkeit des Datenschutzbeauftragten in Hessen vom 20. Mai 2010, GVBl. I S. 208).

Diese Novelle trat am 1. Juli 2010 in Kraft und brachte eine Vielzahl von Änderungen, insbesondere im Zweiten Teil des Hessischen Datenschutzgesetzes (Vorschriften zum Hessischen Datenschutzbeauftragten) und im Fünften Teil (Schlussvorschriften). Die wichtigsten Änderungen sind:

– Übertragung der Aufgabe der Aufsichtsbehörde nach § 38 Abs. 6 BDSG und der Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG und § 16 Abs. 2 Nr. 2 bis 5 Telemediengesetz auf meine Behörde,
– Schaffung einer hauptamtlichen mit B7 bewerteten Position (§ 21 Abs. 6 HDSG) für den Hessischen Datenschutzbeauftragten bei Stärkung der Unabhängigkeit durch Einführung eines besonderen Verfahrens für die Absetzung (§ 21 Abs. 4 HDSG). Der Übergang auf eine hauptamtliche Position ist allerdings erst für meinen Amtsnachfolger vorgesehen (vgl. § 43 Abs. 2 HDSG).

Die Übertragung der Tätigkeit der Aufsichtsbehörde nach § 38 BDSG hat als Folgeregelungen vor allem auch die Zuständigkeit für die Ahndung von Ordnungswidrigkeiten § 24 Abs. 4 HDSG) und die erweiterte Berichtspflicht (§ 30 HDSG) nach sich gezogen (zu den Auswirkungen auf diesen Bericht siehe Ziff. 1.2.3) und eine Umstrukturierung der Behörde erforderlich gemacht (siehe Ziff. 1.2.2).

Die Tätigkeit des Hessischen Datenschutzbeauftragten wird mein Amtsnachfolger künftig als Hauptamt ausüben. Grund hierfür war die mit der Übertragung der Aufgabe der Aufsichtsbehörde nach § 38 BDSG verbundene erheblich höhere Arbeitsbelastung des Hessischen Datenschutzbeauftragten (vgl. LTDrucks. 18/3869 Begründung B zu Nr. 3b aa). Eine Vielzahl von Folgeregelungen ist der Tatsache geschuldet, dass der Hessische Datenschutzbeauftragte kein Beamter ist, sondern ein Amtsträger besonderer Art, der in einem öffentlich rechtlichen Amtsverhältnis steht und auf den deshalb die beamtenrechtlichen Regelungen nicht unmittelbar anwendbar sind.

Die Amtsenthebung ist nach § 21 Abs. 4 HDSG nur in einem speziellen Verfahren im Wege der Klage beim Staatsgerichtshof zu erreichen. Der umfassende Verweis in § 21 Abs. 4 Satz 3 HDSG auf die gängigen beamtenrechtlichen Regelungen steht allerdings nicht mit der von der Richtlinie geforderten Gewährleistung der Unabhängigkeit im Einklang. Für die Position des Hessischen Datenschutzbeauftragten als Amtsträger besonderer Art kann von den in § 21 Abs. 4 Satz 3 HDSG aufgeführten Vorschriften nur § 22 Abs. 1 Nr. 1 und Abs. 2, § 23 Abs. 1 Nr. 1, § 23 Abs. 1 Nr. 3, § 23 Abs. 3 Nr. 1 und § 24 BeamtStG in Betracht kommen; auf diesen Inhalt hätte die Bezugnahme reduziert werden müssen.

Nicht nur wegen der Bereinigung dieses Passus, sondern vor allem wegen der seit langem anstehenden Modernisierung des HDSG ist spätestens anlässlich der durch die Einführung der Befristung veranlassten notwendigen Evaluierung eine Überarbeitung des Gesetzes geboten. Die Arbeiten hierfür sollten möglichst bald aufgenommen werden.

1.2.2
Folgen und Sachstand der Umsetzung in der Dienststelle des HDSB

Der Zeitpunkt des Inkrafttretens des Gesetzes zum 1. Juli 2011 stellte hinsichtlich der Umsetzung der Regelungen eine besondere Herausforderung dar. Der Haushalt für das Jahr 2011 war ohne diese neuen Aufgaben geplant und so waren auch die Personal- und Sachmittel sowie der Stellenplan kalkuliert. Eine Umsetzung von Stellen, Personal- und Sachmitteln aus dem Haushalt des Innenressorts in mein Kapitel war nicht vorgesehen und hätte ohnehin die durch den Aufbau der Behörde in Wiesbaden verursachten Mehrkosten nicht ausreichend abfangen können.

Um eine Weiterführung der Arbeit der Aufsichtsbehörde nach § 38 BDSG sicherzustellen, wurden die bisher im Dezernat Datenschutz beim Regierungspräsidium eingesetzten Mitarbeiterinnen und Mitarbeiter ab 1. Juli 2011 bis zum Jahresende in meine Dienststelle abgeordnet. Da die Beschäftigten weiterhin in Darmstadt bleiben mussten, auch weil bei mir Räumlichkeiten nicht zur Verfügung standen, habe ich eine Außenstelle in Darmstadt betrieben. Insofern war der Status quo des Personalbestandes aufrechterhalten und eine Möglichkeit zum Know-how-Transfer geschaffen. Gleichwohl waren eine Reihe Maßnahmen für die Integration der Außenstelle erforderlich wie die IT-Einbindung, die Telefonintegration, die Installation und Schulung der Beschäftigten für mein Dokumentenmanagement, die Anpassung des Aktenplans auf die hinzugekommenen Aufgaben und die Realisierung des datenschutzgerechten Postaustausches, der ab 1. Juli 2011 über meine Poststelle lief. Außerdem wurden auf oberster Ebene sowie mit den Organisations-, Personal- und Haushaltsdezernaten auf der Arbeitsebene

die Einzelheiten des Vollzuges vereinbart, so z. B. dass zwar die Personalausgaben weiterhin vom Regierungspräsidium, die Reisekosten für Dienstreisen der Mitarbeiter meiner Außenstelle aber von mir zu tragen waren, Dienstaufsichtsbeschwerden gegen Mitarbeiter der Außenstelle – auch wenn sie zurückliegende Zeiträume betrafen – von mir zu bescheiden waren, die Außenstelle als solche kenntlich gemacht wurde. Die Kooperation mit dem Regierungspräsidium war ausgesprochen gut und ich möchte dies auch hier zum Anlass nehmen, mich dafür zu bedanken.

Es war eine Vielzahl von Zusatzarbeit auch in der Außenstelle in Darmstadt zu erledigen wie z. B. die Umsetzung der technischen Maßnahmen der Zusammenlegung, die Einführung des neuen Aktenplans und einer damit verbundenen automatisierten Zählung des Eingabe- und Beratungsvolumens, die Übernahme wichtiger Vorgänge in das Dokumentenmanagementsystem, die Anpassung verschiedener Abläufe bis hin zur Aussonderung von Schriftgut und dem Umzug von Akten, deren Aufbewahrungsfrist noch nicht abgelaufen war, in meine Dienststelle. Für die Arbeiten der Übernahme von Vorgängen in das Dokumentenmanagementsystem habe ich eine Aushilfskraft in dem geringen Umfang, wie mir das im Rahmen der zur Verfügung stehenden Haushaltsmittel möglich war, befristet zur Unterstützung eingestellt.

Daneben war die Dienststelle unter Einbindung des Wissens und der Erfahrungen der langjährigen Leiterin des Dezernates Datenschutz auf eine neue Planorganisation umzustellen, die mit dem Ende der Übergangsphase ab 2012 in Kraft treten sollte und es war nach Zuordnung von „Betreuern“ der neuen Aufgaben in meiner Dienststelle im zweiten Halbjahr des Berichtszeitraumes der Know-how-Transfer zu organisieren.

Erheblichen Zeitaufwand hat auch die vom Hessischen Immobilienmanagement professionell unterstützte Suche nach Räumlichkeiten erfordert, da diese zur Sicherstellung der Synergieeffekte und zur Vermeidung von zusätzlichen Kosten für das Hin- und Herpendeln zwischen Haupthaus und Dependance in möglichst enger räumlicher Nähe zu den derzeitigen Räumen gelegen sein mussten. Die günstige Gelegenheit der Anmietung von Räumen im gleichen Gebäude, die noch etwa ein halbes Jahr vor der Entscheidung über die Übertragung der Aufgabe der Aufsichtsbehörde für den nicht öffentlichen Bereich auf meine Dienststelle bestanden hatte, war zu dem Zeitpunkt der Konkretisierung des Gesetzesvorhabens und des Personalumfangs leider nicht mehr vorhanden. Ein Umzug der Dienststelle insgesamt in neue Räumlichkeiten war wegen des langfristigen Mietvertrages nicht möglich; der Vermieter war zur Auflösung des Vertrages nicht bereit. Nach zähen Verhandlungen wurde für eine Übergangszeit von etwa zwei Jahren eine Fläche im

Nebenhaus angemietet, die aber letztlich den Raumbedarf nicht vollständig befriedigen wird. Diese Lösung soll die Wartezeit abdecken, bis Mietflächen im gleichen Gebäude frei werden (voraussichtlich 2014) und so ggf. die Möglichkeit der Zusammenführung der Dienststelle im gleichen Gebäude besteht. Die Interimsmietfläche wird nicht vor April 2012 zur Verfügung stehen; bis dahin müssen Raumengpässe für die neu übernommenen Beschäftigten durch Übergangslösungen (Auflösung von Sitzungsräumen, Doppelbelegung von Räumen, Anmietung einzelner eingerichteter Arbeitsräume und ggf. externer Sitzungsräume bei einem Anbieter solcher Leistungen im gleichen Haus oder extern) überbrückt werden.

Im Zuge der Aufgabenübertragung war den im Dezernat Datenschutz beim Regierungspräsidium Darmstadt tätigen Beschäftigten zugesagt worden, dass eine Versetzung zum Hessischen Datenschutzbeauftragten nur mit deren Einverständnis vorgenommen werde. Letztendlich konnte ich nur drei Personen für den Wechsel gewinnen. Für die restlichen 13 zu besetzenden Stellen muss Personal über Auswahlverfahren gewonnen werden, die infolge des damit verbundenen erheblichen Arbeitsaufwandes nur sukzessive abgewickelt werden können. Da die Stellenbesetzung und damit die Zusage an ausgewählte Bewerber die Verabschiedung des Haushalts im Parlament voraussetzte, konnte mit den Stellenausschreibungen erst im Herbst begonnen werden. Auf die Auswahlverfahren für die ersten fünf Stellen gingen insgesamt 327 Bewerbungen ein. Drei Stellenbesetzungsverfahren konnten bereits im Berichtszeitraum abgeschlossen werden, die jedoch nur zur Besetzung von zwei Stellen führten, weil eine interne Besetzung ein erneutes Auswahlverfahren für die intern freigewordene Stelle nach sich ziehen muss. Das bedeutet, dass statt der 16 zusätzlichen Stellen mit lediglich fünf besetzten Stellen (eine davon erst zum 1. April 2012) der Aufbau der Behörde mit einer erheblichen Vakanz im Jahr 2012 startet.

Für den Haushalt 2012, der bereits im Berichtszeitraum aufzustellen war, wurden zwar Stellen, Personal- und Sachmittel erhöht, eine solide Planungsbasis gab es aber noch nicht. Dafür waren verschiedene Gründe maßgeblich:

Zum einen war lange Zeit noch nicht klar, wie viele Personen der Aufsichtbehörde in meine Dienststelle wechseln und davon abhängig in welcher Höhe Kosten für die Einstellungsverfahren der restlichen Positionen anfallen und wann die vollen Personalkosten für die zusätzlichen Stellen zu kalkulieren sind.

Zum anderen war die Mietsituation für die neuen Räumlichkeiten unklar, so dass weder die Miete noch zusätzliche Investitionen in die evtl. Mietfläche seriös kalkuliert werden konnten.

Schließlich bestanden auch keine Erfahrungen mit den zu erwartenden Kosten für die zusätzlichen Aufgaben; beim Regierungspräsidium war das Dezernat aufgrund seiner geringen Größe und der Vermeidung kleinteiliger Kostenerfassungen keine eigene Kostenstelle, so dass die bisherigen Kosten als Basis für eine künftige Kalkulation nicht ermittelt werden konnten.

1.2.3
Gemeinsamer Tätigkeitsbericht für den öffentlichen und nicht öffentlichen Bereich

Die Änderung im Datenschutzgesetz hat schließlich dazu geführt, dass ich mit dem 40. Tätigkeitsbericht erstmals gleichzeitig Rechenschaft über die Tätigkeit der Aufsichtsbehörde im nicht öffentlichen Bereich ablege, obgleich diese bis zur Jahresmitte noch nicht in meiner Zuständigkeit lag.

Wegen des durch die Zusammenlegung verursachten zusätzlichen Arbeitsanfalls auch in der Außenstelle standen zwar eigentlich keinerlei freie Kapazitäten für diese Arbeiten zur Verfügung. Dennoch habe ich es für erforderlich gehalten, das Parlament auch über diesen Bereich wenigstens punktuell zu unterrichten. Der Auffassung der Landesregierung, ein inhaltlicher Bericht sei nicht mehr nötig (vgl. 24. Bericht über die Tätigkeit der Aufsichtsbehörde für den nicht öffentlichen Bereich, LTDrucks. 18/4569, Ziff. 6), weshalb ausschließlich statistische Angaben mitgeteilt wurden, kann ich mich nicht anschließen. Entgegen dieser Ansicht ist der Sinn der Berichtspflicht über den Datenschutz im nicht öffentlichen Bereich dem Parlament gegenüber nicht die Eröffnung von Einflussnahmen auf die Arbeit der Aufsichtsbehörde: Eine solche Einwirkung war nach der EG-Datenschutzrichtlinie nie zulässig (vgl. Entscheidung des EuGH vom 14. März 2010 - C-518/07 - NJW 2010, 1265). Die Berichtspflicht besteht auch nicht zu dem Zweck, der Wirtschaft eine Richtschnur für die Praxis der Aufsichtsbehörde bekannt zu geben – dazu ist die Installation einer Berichtspflicht dem Parlament gegenüber eher nicht geeignet. Zweck dieser Berichtspflicht ist vielmehr die Herstellung des Informationsgleichgewichts zwischen Regierung und Parlament. Künftig dient die Berichtspflicht auch dazu, die unabhängige Stellung des Datenschutzbeauftragten verfassungskonform auszugestalten. Für das Parlament gibt es auch außerhalb der – unzulässigen – Einflussnahme auf die Aufsichtsbehörde Reaktionsmöglichkeiten auf Inhalte des Berichts: So könnte es z. B., wenn aus dem Bericht Fehlentwicklungen des Datenschutzrechtes absehbar sind, mit einen Antrag nach § 27 der Geschäftsordnung des Hessischen Landtags die Landesregierung zum Handeln auffordern, denn diese könnte z. B. über eine Bundesratsinitiative Einfluss auf die Bundesgesetzgebung nehmen.

Ich habe deshalb den anderen Weg gewählt. Wegen der Umstellung auf eine gemeinsame automationsunterstützte Zählung ab Mitte des Berichtszeitraums habe ich auf die Übermittlung von statistischen Werten für 2011 verzichtet und berichte statt dessen über die Arbeit der Aufsichtsbehörde in zwei exemplarischen Beispielen, weil ich die inhaltliche Berichterstattung an das Parlament für wesentlich halte.

Die Verbindung beider Berichtspflichten hat einen neuen Aufbau des Tätigkeitsberichtes nach sich gezogen. Die endgültige Form wird noch zu finden sein. Klar ist jedoch, dass eine Stellungnahme der Landesregierung nur zu den Teilen des Berichtes erforderlich ist, die – zumindest auch – Problemstellungen des öffentlichen Bereichs betreffen. Das wird in aller Regel die gemeinsamen Bereiche wie technische Fragestellungen, eine Vielzahl von Fragen im Gesundheits- und Bankenbereich, aber auch im Bereich der Daseinsvorsorge betreffen, wo die Problemstellungen gleichermaßen öffentliche Stellen wie nicht öffentliche Stellen betreffen.

Für diesen Berichtszeitraum habe ich in Ziff. 5 die Fragestellungen im nicht öffentlichen Bereich aufgegriffen und in Ziff. 10 die Beschlüsse des Düsseldorfer Kreises, die ausschließlich den nicht öffentlichen Bereich betreffen, wiedergegeben.

Die gleich lautenden Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und Beschlüsse des Düsseldorfer Kreises sind in Ziff. 9 zusammengefasst.

Letztendlich sind die in Ziff. 5.1 geschilderten datenschutzrechtlichen Probleme des elektronischen Lastschriftverfahrens auch für den öffentlichen Bereich relevant, weil sie in gleichem Maße auch Grundlagen für die Sparkassen als öffentliche Stellen betreffen. Insofern ist dieser Tätigkeitsbericht auch schon ein Spiegel der Synergieeffekte.

1.2.4
Auswirkung der Rechtsänderungen auf die Zusammenarbeit auf Bund-/Länderebene

Mit Ausnahme von Bayern sind in allen Bundsländern bis zum Ende des Berichtszeitraums die Kontrollstellen für den öffentlichen und nicht öffentlichen Datenschutz bei den Datenschutzbeauftragten zusammengefasst. Dies bedeutet auch, dass die noch bestehenden Doppelstrukturen für den Erfahrungsaustausch, die Koordinierung und Abstimmung in Einzelfragen abgebaut werden sollten. Ansätze hierzu wurden im Berichtszeitraum bereits begonnen. Dies werde ich im kommenden Jahr mit meinen Kollegen im Bund und in den Ländern weiter verfolgen.

1.3
Einordnung des Datenschutzes

1.3.1
Allgemeines

Die Einordnung des Datenschutzes wurde bereits in den vorangegangenen Tätigkeitsberichten ausführlich gewürdigt. Hierauf wird verwiesen. Groß Neues ist nicht nachzutragen. Auch im Berichtszeitraum zeigte sich die Leistungsfähigkeit der Verankerung der informationellen Selbstbestimmung in Art. 1 Abs. 1 und Art. 2 Abs. 1 GG. Die Kombination beider Grundrechte macht einerseits die Menschenwürde in ihren Grenzbereichen abwägbar und bestärkt andererseits die allgemeine Handlungsfreiheit. Der Datenschutz bewegt sich auf einer gleitenden Skala zwischen zwei Eckpunkten. Das bedeutet aber auch, dass diese Eckpunkte einmal erreicht werden können. So ist der Kernbereich der privaten Lebensgestaltung absolut geschützt. Andererseits kann die informationelle Selbstbestimmung auch allein auf die allgemeine Handlungsfreiheit gestützt sein.

So wurde vom Bundesverfassungsgericht durch Kammerbeschluss vom 1. Februar 2011 (2 BvR 1236/10) die Verfassungsbeschwerde gegen die Offenlegungspflicht eines Jahresabschlusses einer GmbH, die auf das Recht auf informationelle Selbstbestimmung gestützt war, verworfen. Auffällig ist, dass die informationelle Selbstbestimmung in diesem Beschluss nur auf Art. 2 Abs. 1 GG gestützt wurde. In weiteren Kammerbeschlüssen wurde diese Rechtsprechung bestätigt.

Praktisch wesentlich bedeutsamer ist der Kammerbeschluss vom 20. Mai 2011 (2 BvR 2072/10), der aus der illegalen Videoaufzeichnung eines Verkehrsverhaltens kein Beweisverwertungsverbot in einem Bußgeldverfahren ableitete. Der Beschwerdeführer war auf der Bundesautobahn A 5 dabei gefilmt worden, als er bei einer Geschwindigkeit von 145 km/h den Sicherheitsabstand von 60,40 m unterschritt. Das Regierungspräsidium Kassel hatte gegen den Beschwerdeführer einen Bußgeldbescheid festgesetzt und die Eintragung von zwei Punkten im Verkehrszentralregister angeordnet. Den dagegen gerichteten Einspruch hatte der Beschwerdeführer damit begründet, er sei nicht als Fahrer zu identifizieren. Es liege ein Verstoß gegen die Entscheidung des Bundesverfassungsgerichts vom 11. August 2009 (2 BvR 941/08) vor. Er blieb bei den Instanzgerichten ohne Erfolg und legte hiergegen Verfassungsbeschwerde ein. Das Bundesverfassungsgericht nahm die Verfassungsbeschwerde nicht an, da die Verwendung der Videoaufzeichnung zum Nachweis des Abstandsverstoßes nicht den absoluten Kernbereich der privaten Lebensgestaltung des Beschwerdeführers oder dessen

Privatsphäre berühre. Der Beschwerdeführer habe sich vielmehr durch seine Teilnahme am öffentlichen Straßenverkehr selbst der Wahrnehmung und der Beobachtung durch andere Verkehrsteilnehmer und auch der Kontrolle seines Verhaltens im Straßenverkehr durch die Polizei ausgesetzt. Hinzu komme, dass der aufgezeichnete und festgehaltene Lebenssachverhalt des Beschwerdeführers auf einen sehr kurzen Zeitraum begrenzt sei. Diese Rechtsprechung bestätigt die Prognose, dass das Bundesverfassungsgericht die Verteidigungslinie vor dem Grundrecht auf Datenschutz soweit vorgezogen hatte, dass es alsbald zu einer Frontbegradigung gezwungen sein würde. Privatheit bedeutet nicht Isoliertheit. Wer sich Hoffnungen macht, aus der Rechtsprechung des Bundesverfassungsgerichts einen absoluten Schutz gegen Vorratsdatenspeicherung, Online-Durchsuchungen und dergleichen begründen zu können, sieht sich wieder auf den Boden der verfassungsrechtlichen Normalität zurückversetzt. Dies gilt erst recht für den Beschluss des Bundesverfassungsgerichts vom 12. Oktober 2011 (2 BvR 236/08, 2 BVR 237/08, 2 BvR 422/08), der die Verfassungsmäßigkeit von Vorschriften des Gesetzes zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 (BGBl. I S. 3198) bestätigte. Mit diesem Gesetz sollte nach dem Willen der Bundesregierung ein harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmaßnahmen geschaffen und die Anforderung des Urteils des Bundesverfassungsgerichts vom 27. Juli 2005 (1 BvR 668/04, BVerfGE 113, 348) erfüllt werden. Auch aus Sicht des Bundesverfassungsgerichts ist dies dem Gesetzgeber gelungen. Die Unterlassung der Benachrichtigung von verdeckten Ermittlungsmaßnahmen sei an besonders strenge Voraussetzungen geknüpft (Art. 10 Abs. 1 GG). Es wurden zwar die Bedingungen einer freien Telekommunikation aufrechterhalten, in dieses Grundrecht dürfe aber eingegriffen werden. Auch in dieser Entscheidung setzt sich das Bundesverfassungsgericht mit dem Kernbereichsschutz auseinander. Dabei vermeidet es zu Recht die Verabsolutierung des Grundrechtschutzes und betont: „Bestehen im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, hat sie grundsätzlich zu unterbleiben (BVerfGE 120, 274, 338). Anders liegt es jedoch, wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern.“ Bei realistischer Sichtweise kann die Lösung der Kernbereichsproblematik nicht auf der Ebene der Erhebung, sondern erst auf der Ebene der Verwertung gefunden werden. Bei einer derartigen pragmatischen Sicht der Kernbereichssphäre steht nichts entgegen, den Schutz des Kernbereichs aus der Wohnung in den Sozialbereich auszudehnen. Erst wenn das gelungen ist, ist die informationelle Selbstbestim-

mung mehr als nur Gewährleistung von Privacy. Selbst dann ist zu berücksichtigen, dass es sich um ein abwägungsfähiges Grundrecht handelt, das mit höheren oder mit mindestens gleichrangigen Grundrechtspositionen in Kollision geraten kann. Dies bestätigt (wieder einmal) der Kammerbeschluss des Bundesverfassungsgericht vom 8. Dezember 2011 (1 BvR 927/08), mit dem der Verfassungsbeschwerde der Zeitschrift „BUNTE“ stattgegeben wurde, der durch Einstweilige Verfügung des Landgerichts Berlin und des Kammergerichts eine bestimmte Wortberichterstattung aufgegeben worden war. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG biete nicht schon davor Schutz, überhaupt in einem Bericht individualisierend benannt zu werden. Dabei komme es vor allem auch auf den Inhalt der Berichterstattung an. Das allgemeine Persönlichkeitsrecht schütze insoweit freilich insbesondere auch vor einer Beeinträchtigung der Privat- oder Intimsphäre. Ein von dem Kommunikationsinhalt unabhängiger Schutz sei bei Textberichterstattung hingegen nur unter dem Gesichtspunkt des Rechts am geschriebenen Wort anerkannt. Gewährleistet sei jedoch nicht, dass der Einzelne nur so dargestellt werde und nur dann Gegenstand öffentlicher Berichterstattung werden könne, wenn und wie er es wünsche.

1.3.2 Publikationen

Im Lichte dieser Rechtsprechung des Bundesverfassungsgerichts sind zahlreiche Publikationen zum Datenschutz im Berichtszeitraum teilweise überholt, aber natürlich nicht bedeutungslos. Zu erwähnen sind insbesondere die Schrift von Kühlin/Seidel/Sevreds, Datenschutzrecht 2. Auflage 2011 und der Bericht von Gola „Die Entwicklung des Datenschutzrechts in den Jahren 2010/2011“, NJW 2011, 2484 ff. Eine ausführliche Darstellung zum Dauerbrenner der Videoüberwachung bietet Siegel „Spiel ohne Grenze?, grundrechtliche Schranken der Videoüberwachung durch öffentliche Stellen und private“, VerwArch 2011, 59 ff. sowie AbatE „Präventive und repressive Videoüberwachung öffentlicher Plätze“, DuD 2011, 451 ff. Zu erwähnen ist weiter Möstel „Vorratsdatenspeicherung, wie geht es weiter?“, ZRP 2011, 225 ff. und von Herrmann/Soiné „Durchsuchung persönlicher Daten auf Grundrechtsschutz“, NJW 2011, 2922 ff. Erwähnt sei schließlich Ronellenfitsch „Abschied vom Trennungsgebot im Landesamt für Verfassungsschutz Hessen“, Verfassungsschutz in der freiheitlichen Demokratie 2011 S. 71 ff.

2. Europa

2.1
Gemeinsame Kontrollinstanz für das Schengener Informationssystem

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrnehmung der Interessen der Landesdatenschutzbeauftragten in der Europäischen Kontrollinstanz für das Schengener Informationssystem übertragen. Meine Mitarbeiterin ist im Berichtszeitraum als Vorsitzende der Kontrollinstanz wiedergewählt worden. Der Beitrag stellt die Arbeitsschwerpunkte der Sitzungen der Kontrollinstanz im Jahr 2011 dar.

2.1.1
Schengener Informationssystem der zweiten Generation (SIS II)

Im 39. Tätigkeitsbericht (Ziff. 2.3.1) hatte ich berichtet, dass sich der Zeitrahmen für die Realisierung des SIS II immer weiter verlängert. Auch nach positiver Einschätzung sollte nach damaliger Sicht das SIS II vor Mitte des Jahres 2013 nicht betriebsbereit sein. Mittlerweile wird auch ein Start im Jahr 2013 skeptisch gesehen.

Die Gemeinsame Kontrollinstanz (GK) bereitet derzeit eine Kontrolle des zentralen Teils des SIS (CSIS) in Straßburg vor. Dabei soll auch geprüft werden, ob die Voraussetzungen für einen Test des SIS II mit Echtdaten aus datenschutzrechtlicher Sicht vorliegen. Die Kontrolle soll im ersten Halbjahr 2012 von einem aus technischen Sachverständigen aus sechs Mitgliedsstaaten bestehenden Team durchgeführt werden.

2.1.2
Gemeinsame Überprüfung der Ausschreibungen zur Festnahme

Die im 39. Tätigkeitsbericht (Ziff. 2.3.3) erwähnte gemeinsame Überprüfung der Ausschreibungen nach Art. 95 SDÜ ist derzeit im Gang. Es geht dabei um die Ausschreibung im SIS von Personen, die wegen einer Straftat mit Haftbefehl zur Verfolgung oder zur Vollstreckung gesucht werden.

> *Art. 95 Abs. 1 SDÜ*
>
> *Daten in Bezug auf Personen, um deren Festnahme mit dem Ziel der Auslieferung ersucht wird, werden auf Antrag der Justizbehörde der ersuchenden Vertragspartei aufgenommen.*

In Deutschland liegen der Ausschreibung im SIS immer ein durch den Richter ausgestellter nationaler Haftbefehl sowie ein von der Staatsanwaltschaft

erlassener Europäischer Haftbefehl (European Arrest Warrant, EAW) zugrunde. Der EAW dient vor allem dem Zweck, dass im Falle einer Festnahme der gesuchten Person in einem anderen europäischen Land die Auslieferung einfacher und schneller erfolgen kann.

Die GK hat als Grundlage für die Überprüfung in allen Schengen-Ländern einen detaillierten Fragebogen entwickelt. Derzeit sind der Bundesbeauftragte für den Datenschutz und Informationsfreiheit für seinen Zuständigkeitsbereich sowie ich dabei, die erforderlichen Informationen beim BKA, dem HLKA, den Gerichten und Staatsanwaltschaften einzuholen. Gleichzeitig werden von mir in Hessen stichprobenartig Überprüfungen von Akten zu Personen, die nach Art. 95 SDÜ im SIS ausgeschrieben sind, durchgeführt.

2.1.3
Veränderung des Zugriffs von EUROPOL auf das SIS

Bereits seit einigen Jahren hat Europol nach Art. 101a SDÜ Zugriff auf verschiedene Ausschreibungen im SIS.

> *Art. 101a Abs. 1 SDÜ*
>
> *Das Europäische Polizeiamt (EUROPOL) hat im Rahmen seines Mandats und auf eigene Kosten Zugriff auf die nach den Art. 95, 99 und 100 im SIS gespeicherten Daten mit dem Recht, diese unmittelbar abzurufen.*

Dieser Zugriff soll nunmehr nicht mehr wie bisher durch eine getrennte webbasierte Datenleitung erfolgen. Die Mitarbeiter bei EUROPOL sollen vielmehr jetzt von ihrem PC aus, mit dem sie auf das EUROPOL-System zugreifen, auch auf das SIS Zugriff haben. Statt der bisher erfolgenden physikalischen Trennung soll es jetzt also nur noch eine logische geben. Die GK hat deshalb die Frage zu entscheiden, ob das von EUROPOL geplante Vorhaben mit Art. 101a Abs. 6 vereinbar ist.

> *Art. 101a Abs. 6 SDÜ*
>
> *Europol ist verpflichtet,*
>
> *...*
>
> *b) unbeschadet der Abs. 4 und 5 es zu unterlassen, Teile des SIS, zu denen es Zugang hat, oder die hierin gespeicherten Daten, auf die es Zugriff hat, mit einem von oder bei EUROPOL betriebenen Computersystem für die Datenerhebung und -verarbeitung zu verbinden bzw. in ein solches zu übernehmen oder bestimmte Teile des SIS herunterzuladen oder in anderer Weise zu vervielfältigen.*

Damit verfolgt Art. 101a Abs. 6 ein wichtiges Ziel: Das Herunterladen oder Kopieren von Daten aus dem SIS soll unterbunden werden. Es sollen aber

auch Gefährdungen ausgeschlossen werden, die sich aus einer physikalischen Vermengung von Daten aus dem SIS mit Daten, die sich in von EUROPOL betriebenen Datenverarbeitungssystemen befinden, ergeben. Voraussetzung für eine Realisierung des von EUROPOL geplanten Vorhabens ist aus Sicht der GK, dass ausreichende technische Garantien bestehen, dass eine derartige Verbindung von Daten ausgeschlossen ist.

2.2

Gemeinsame Kontrollinstanz für EUROPOL

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

2.2.1

Einbeziehung von EUROPOL in das SWIFT-Abkommen mit den USA

Im 39. Tätigkeitsbericht (Ziff. 2.4.2) hatte ich von dem sog. SWIFT- bzw. TFTP-Abkommen (Terrorist Finance Tracking Program) zwischen der EU und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der EU an die USA berichtet. EUROPOL hat nach diesem Abkommen die Aufgabe, Ersuchen amerikanischer Behörden um Übermittlung von Zahlungsverkehrsdaten an den Dienstleister SWIFT, auf ihre Konformität mit dem TFTP-Abkommen zu überprüfen.

Da im Zusammenhang mit der Einbindung von EUROPOL in diese Datenübermittlungen eine Reihe von Fragen auftauchten, hat die Gemeinsame Kontrollinstanz (GKI) einen Kontrollbesuch zu diesem Thema bei EUROPOL vorgenommen.

Im Rahmen der Kontrolle sollte u. a. überprüft werden, ob die von den USA beantragten Übermittlungen von SWIFT-Daten gemäß der im TFTP-Abkommen festgelegten Bedingungen erforderlich und verhältnismäßig sind. Die mit der Überprüfung beauftragte Arbeitsgruppe der GKI stellte fest, dass die bei Europol eingegangenen schriftlichen Anträge der USA zu allgemein und zu abstrakt waren, um die korrekte Bewertung der Notwendigkeit der beantragten Datenübermittlungen zu ermöglichen. EUROPOL hat darauf hingewiesen, dass mündliche Informationen eine wichtige Rolle bei der Überprüfung jeder Abfrage spielen. Diese Informationen erhalten bestimmte EUROPOL-Bedienstete von den USA unter der Bedingung,

dass keine Aufzeichnungen gemacht werden. Eine ordnungsgemäße Überprüfung, ob die Anfragen mit dem TFTP-Abkommen im Einklang stehen und daher zutreffender Weise von EUROPOL genehmigt worden sind, war daher nicht möglich. Die GKI hat daher die Empfehlung ausgesprochen, das Verfahren für die Genehmigung von Anträgen der USA so zu verändern, dass es sowohl dem Datenschutzbeauftragten von EUROPOL als auch der GKI möglich ist, die Entscheidungen von Europol zu überprüfen (s. Ziff. 8.4).

2.2.2

Neues Konzept für Analysearbeitsdateien

Eines der wichtigsten Vorhaben von EUROPOL ist ein neues Konzept für die bei EUROPOL betriebenen Analysearbeitsdateien. EUROPOL verfolgt dabei das Ziel, die in Analysearbeitsdateien gespeicherten Daten in einer effizienteren Weise zu nutzen, die der Komplexität der Kriminalität und der Überschneidung einzelner Kriminalitätsbereiche besser gerecht wird.

Die Speicherung in Analysearbeitsdateien ist die für die Arbeit von EUROPOL bedeutendste Art der Datenverarbeitung.

Art. 14 EUROPOL-Beschluss

(1) Soweit dies zur Wahrnehmung seiner Aufgaben erforderlich ist, kann EUROPOL in Arbeitsdateien zu Analysezwecken Daten über in seine Zuständigkeit fallende Straftaten einschließlich Daten über damit im Zusammenhang stehende Straftaten gemäß Art. 4 Abs. 3 speichern, ändern und nutzen. ...

Die in Analysearbeitsdateien gespeicherten Daten dienen der Zusammenstellung, Verarbeitung und Nutzung von Daten zur Unterstützung der kriminalpolizeilichen Ermittlungen.

Bisher gab es etwa 23 derartige Analysearbeitsdateien, wie z. B. für die Geldwäsche, den Rauschgift- und Kokainhandel, die Kinderpornografie, die Zahlungskartenkriminalität, den Menschenhandel, den Zigarettenschmuggel etc.

Nunmehr plant EUROPOL die 23 Arbeitsdateien auf eine Datei betreffend „organisierte Kriminalität“ und eine andere Datei mit dem Titel „Bekämpfung des Terrorismus“ zu reduzieren. Erreicht werden soll damit u. a., dass die zuständigen Mitarbeiter zunächst nicht nur auf die ihnen zugeordnete Datei (z. B. Menschenhandel) zugreifen können, sondern auf den gesamten Bereich der organisierten Kriminalität. Zwar soll der Zugriff an den Erforderlichkeitsgrundsatz gebunden werden, dennoch wird damit ein viel breiterer Zugriff unter einfacheren Voraussetzungen ermöglicht.

Die GKI wurde frühzeitig in das Vorhaben einbezogen und die betreffende Arbeitsgruppe der GKI, in der meine Mitarbeiterin vertreten ist, hat mehrfach Treffen mit EUROPOL zu diesem Thema durchgeführt.

Die Zusammenführung aller bisherigen Analysearbeitsdateien in nur zwei Dateien „organisierte Kriminalität“ und „Bekämpfung des Terrorismus“ wirft insbesondere die Frage auf, wie dabei die bisherigen für die einzelnen Analysearbeitsdateien festgelegten Regelungen zu Zweckbestimmung, Prüf- und Löschfristen oder zur Information der GKI über eine neue Datei beibehalten werden können. Nach dem Wortlaut des EUROPOL-Beschlusses gelten diese datenschutzrechtlichen Bestimmungen für die jeweilige Analysearbeitsdatei, d. h. – falls das Projekt umgesetzt wird – nur für die beiden umfangreichen Datensammlungen. Damit würden die Datenschutzregelungen aber weitgehend ins Leere laufen. Deshalb muss rechtlich bindend sichergestellt werden, dass die einschlägigen und auf die einzelnen Kriminalitätsbereiche abgestimmten Datenschutzbestimmungen weiterhin gelten.

Die Arbeitsgruppe der GKI hat diese Forderungen EUROPOL vorgetragen und steht in laufenden Gesprächen.

2.2.3
Kontrolle von EUROPOL

Die GKI hat im Jahr 2011 wieder eine Kontrolle bei EUROPOL durchgeführt. Der Bericht über diese Kontrolle ist vertraulich.

2.3
EU-System zum Aufspüren der Terrorismusfinanzierung

Die Europäische Kommission hat eine Mitteilung zur Errichtung eines europäischen Systems zur Aufspürung von Terrorismusfinanzierung (Terrorist Finance Tracking System/TFTS) veröffentlicht, mit der sich die Artikel 29-Gruppe kritisch auseinandergesetzt hat.

Als der Rat der Europäischen Union dem TFTP-Abkommen der Kommission mit den USA zustimmte, verband er das mit der Aufforderung, spätestens ein Jahr nach dem Inkrafttreten des Abkommens *„einen rechtlichen und technischen Rahmen für die Extraktion der Daten auf dem Gebiet der Europäischen Union“* (ABl. L195 vom 27. Juli 2010, S. 3) vorzulegen. Die Idee, die hinter diesem Auftrag stand, war, die Extraktion der für die Terrorismusbekämpfung relevanten Zahlungsdaten auf europäischem Grund stattfinden zu lassen und so die Übermittlung von großen Mengen ungefilterter Datenpakete in die USA zu vermeiden.

Als erste Reaktion auf diesen Auftrag hat die Kommission im Juli 2011 eine Mitteilung veröffentlicht, in der sie zunächst drei Optionen für ein EU-System zum Aufspüren der Terrorismusfinanzierung zur Diskussion stellt. Da die Beschreibung dieser drei Optionen noch sehr allgemein gehalten ist, hat sich die Artikel 29-Gruppe (unabhängiges Beratungsgremium der Europäischen Kommission in Datenschutzfragen, in dessen zuständiger Untergruppe ich mit einer Mitarbeiterin vertreten bin) ebenfalls auf grundsätzliche Hinweise zu einem TFTS-Projekt beschränkt.

Im Wesentlichen problematisiert die Artikel 29-Gruppe Folgendes:

Nach der derzeit geltenden Rechtslage ist bereits fraglich, auf welche Rechtsgrundlage die Errichtung eines solchen europäischen Systems gestützt werden könnte. Diese Frage bedarf der Klärung noch bevor Entscheidungen über die konkrete Ausgestaltung des Systems getroffen werden können.

Darüber hinaus stellt die Artikel 29-Gruppe in Frage, ob ein TFTS – unabhängig von der jeweiligen Ausprägung – überhaupt den Erfordernissen der Erforderlichkeit und der Verhältnismäßigkeit der Datenverarbeitung gerecht wird. Die Gruppe stellt fest, dass es hierfür jedenfalls nicht ausreichend ist, wenn ein solches System lediglich einen Zusatznutzen im Kampf gegen Terrorismus bringt. Darüber hinaus müsste der Eingriff in das Recht auf informationelle Selbstbestimmung, der durch den Betrieb eines TFTS verursacht wird, in einem angemessenen Verhältnis zu dem hierdurch erzielten Sicherheitsgewinn stehen.

Schließlich besteht eine Forderung der Artikel 29-Gruppe darin, die Überlegungen zu einem TFTS eng mit der Frage nach dem Schicksal des bestehenden TFTP-Abkommens mit den USA zu verknüpfen. Es wäre aus der Sicht des Datenschutzes nichts gewonnen, wenn das TFTS, das eigentlich das TFTP-Abkommen mit den USA ersetzen und das Verfahren datenschutzfreundlicher gestalten sollte, als weiteres Instrument der Terrorismusbekämpfung eingeführt würde und daneben das TFTP-Abkommen unverändert weiterbestünde.

3. Hessen

3.1 Querschnitt

3.1.1
Diskussion um ein Hessisches Korruptionsbekämpfungsgesetz

Der Hessische Landtag hat im April 2011 den Entwurf der SPD-Fraktion für ein Gesetz zur Verbesserung der Korruptionsbekämpfung und zur Errichtung und Führung eines Korruptionsregisters (Hessisches Korruptionsbekämpfungsgesetz; LTDrucks. 18/3005) abgelehnt (LTDrucks. 18/3908 u. Plenarprotokoll 18/71 13. April 2011 S. 4921 bis 4928). Mit dem Gesetz wollte die SPD-Fraktion das gegenwärtig aufgrund eines Erlasses von der OFD betriebene Melde- und Informationssystem für Vergabesperren auf eine gesetzliche Grundlage stellen und ausweiten. Im Rahmen einer vom Ausschuss für Wirtschaft und Verkehr zu dem Gesetzentwurf durchgeführten Anhörung habe ich mich zu den datenschutzrechtlichen Anforderungen eines Korruptionsregistergesetzes geäußert.

3.1.1.1
Gegenwärtiges Melde- und Informationssystem

In Hessen existiert seit 1995 für die Behörden des Landes ein Melde- und Informationssystem für Vergabesperren (Gemeinsamer Runderlass der Landesministerien vom 14. November 2007, StAnz S. 2327). Bei der Oberfinanzdirektion Frankfurt ist eine Melde- und Informationsstelle eingerichtet. Hat eine Behörde einen Bewerber wegen schwerer Verfehlungen, die seine Zuverlässigkeit in Frage stellen, von der Teilnahme am Wettbewerb ausgeschlossen, teilt sie dies der Melde- und Informationsstelle bei der OFD mit. Die Mitteilung der Vergabesperre umfasst folgende Daten: Behörde, die den Ausschluss ausgesprochen hat, Datum, Aktenzeichen, Name eines Ansprechpartners, Telefonnummer des Ansprechpartners, Umfang der Sperre, betroffenes Unternehmen, Gewerbezweig/Branche, Anschrift und – falls bekannt – die Handelsregisternummer. Bei geplanten Vergaben über einem Schwellenwert von 15.000 Euro bei Dienstleistungen und 25.000 Euro bei Bauaufträgen hat sich die Vergabestelle vor der Vergabe bei der Melde- und Informationsstelle zu erkundigen, ob die für die Vergabe in Aussicht genommene Firma vom Wettbewerb ausgeschlossen ist.

Laut Mitteilung der OFD vom 2. Februar 2011 waren in Hessen Anfang des Jahres 2011 ca. 20 Unternehmen und freiberuflich Tätige vom Wettbewerb ausgeschlossen. 12 Unternehmer bzw. Unternehmen befanden sich in einem Anhörungsverfahren. Insgesamt wurden in den vergangenen zehn

Jahren 242 Anhörungsverfahren durchgeführt und 115 Unternehmen oder freiberuflich Tätige für den Wettbewerb gesperrt.

Ähnlich wie Hessen verfahren Baden-Württemberg (Verwaltungsvorschrift der Landesregierung und der Ministerien zur Korruptionsverhütung und -bekämpfung vom 19. Dezember 2005 – GABl. 2006, S. 125) und Rheinland-Pfalz (Bekämpfung der Korruption in der öffentlichen Verwaltung. Verwaltungsvorschrift der Landesregierung vom 7. November 2000 i. d. F. vom 29. April 2003 – FM – O 1559 A – 411).

Datenschutzrechtlich handelt es sich bei diesem Melde- und Informationssystem um ein gemeinsames Verfahren gemäß § 15 HDSG. Verantwortlich für die Datenverarbeitung sind die Behörden, welche die Vergabesperre ausgesprochen haben. Sowohl die Datenspeicherung als auch die Datenübermittlung an die anfragenden Vergabestellen erledigt die OFD im Auftrag der Behörden, welche die Vergabesperre ausgesprochen haben. Deshalb benötigt das gegenwärtige Melde- und Informationssystem keine bereichsspezifische gesetzliche Regelung, sondern es genügen die allgemeinen Verarbeitungsvorschriften des HDSG.

Der Gesetzentwurf der Fraktion der SPD sah im Unterschied zum gegenwärtigen Melde- und Informationssystem in Hessen eine weitergehende Lösung vor, bei der die OFD als Register führende Stelle nicht mehr im Auftrag der Behörden, die die Vergabesperre verhängt haben, tätig geworden wäre, sondern als selbständige Daten verarbeitende Stelle. Auch Inhalt und Anwendungsbereich des Registers sollten erheblich ausgeweitet werden. Für ein solches Register wäre das HDSG keine ausreichende Rechtsgrundlage, sondern es bedürfte einer bereichsspezifischen gesetzlichen Regelung.

3.1.1.2
Zulässigkeit eines Korruptionsregisters

Die zentrale Erhebung, Speicherung und Übermittlung von Daten über Rechtsverstöße und ausgesprochene Vergabesperren ist ein Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Unternehmer (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Das Recht auf informationelle Selbstbestimmung existiert nicht schrankenlos. Eingriffe sind im überwiegenden Allgemeininteresse zulässig. Der Gesetzentwurf der SPD-Fraktion ging zu Recht davon aus, dass Korruption eine Bedrohung der wesentlichen Grundlagen unserer Gesellschaft sei. Korruptionsbekämpfung mittels Vergabesperren und einem zentralisierten Informationssystem können als im überwiegenden Allgemeininteresse zu treffende Maßnahmen angesehen wer-

den. Unternehmen, die sich als unzuverlässig erwiesen haben, sollten keine öffentlichen Aufträge erhalten. Das Risiko eines Ausschlusses vom Wettbewerb und der Eintragung im Korruptionsregister setzt die Unternehmen unter erheblichen Druck, sich rechtskonform zu verhalten, nach dem Motto: Wettbewerbswidriges Verhalten bei der Bewerbung um öffentliche Aufträge lohnt sich nicht. Die Behörden, die im Vergabeverfahren über die Zuverlässigkeit oder Unzuverlässigkeit eines Bieters entscheiden müssen, benötigen dazu möglichst umfassende und verlässliche Daten. Ein zentrales Register, in dem einschlägige Straftaten und andere Rechtsverstöße sowie Vergabesperren erfasst werden, auf das die Vergabestellen zugreifen können, erscheint als besonders geeignete Informationsquelle. Es sind außerdem keine gleich effektiven aber weniger einschneidenden Mittel ersichtlich. Ein Rückgriff auf das Gewerbezentralregister (§§ 150a GewO) liefert lediglich Informationen über die gewerberechtliche Zuverlässigkeit, im Vergabeverfahren geht es jedoch um die wettbewerbsrechtliche Zuverlässigkeit. Das staatsanwaltliche Verfahrensregister (§§ 492 ff. StPO) oder das Bundeszentralregister (§§ 4 ff. BZRG) sind ebenfalls keine Register mit gleichermaßen umfassenden Informationen.

3.1.1.3
Verfassungskonforme Ausgestaltung

Ein Korruptionsregistergesetz sollte den Zweck der Datenverarbeitung festlegen und die Aufgaben und Befugnisse der beteiligten Stellen, das Erhebungsverfahren, die Speicherungsbedingungen einschließlich Löschungsfristen, die Datenübermittlung aus dem Register, Benachrichtigungspflichten sowie Auskunfts-, Berichtigungs- und Löschungsansprüche der Betroffenen regeln.

Der Gesetzentwurf der SPD-Fraktion erfüllte weitgehend diese Anforderungen. Der Verarbeitungszweck war hinreichend bestimmt. Das Register sollte der Sammlung und Bereitstellung von Informationen über die Unzuverlässigkeit von natürlichen und juristischen Personen (§ 1 Abs. 1) mit dem Ziel der Unterstützung der Prüfung der Zuverlässigkeit von Bietern und Bewerbern und der Strafverfolgungsbehörden (§ 1 Abs. 2) dienen.

Der zentralen Informationsstelle sollte die Führung des Korruptionsregisters obliegen. Sie sollte keine Entscheidung über Vergabeausschlüsse treffen (§ 3 Abs. 1). Unklar blieb jedoch, ob die zentrale Informationsstelle das Vorliegen der Speicherungsvoraussetzungen zu überprüfen hatte. § 5 Abs. 5 übertrug der meldenden Stelle die Verantwortung für die Richtigkeit der mitgeteilten Daten und § 6 Abs. 1 verlangte von der zur Mitteilung verpflichteten Behörde bei Vorliegen der Eintragungsvoraussetzungen eine Datenübermittlung an das Register. Daraus hätte man schließen können, dass die Informationsstelle im Hinblick auf die Erhebung und Speicherung der Registerdaten keine eigenen Prüfpflichten haben sollte. Als verantwortliche Stelle müsste der zentralen Informationsstelle jedoch eine Prüfkompetenz eingeräumt werden. Ich habe daher eine entsprechende Klarstellung im Gesetz empfohlen und angeregt, zu regeln, wo die Informationsstelle errichtet werden soll. In der Begründung des Gesetzentwurfs (S. 10) wurde ein Ausbau der von der OFD Frankfurt betriebenen Melde- und Informationsstelle für Vergabesperren befürwortet.

Der Gesetzentwurf sah vor, neben Straftaten und Verstößen (§ 4 Abs. 1) Vergabeausschlüsse, die im Zusammenhang mit meldepflichtigen Rechtsverstößen verhängt worden sind (§ 4 Abs. 3), im Korruptionsregister zu speichern. Welche Delikte bei der Prüfung der Zuverlässigkeit herangezogen werden dürfen, z. B. Kriterien, die von der gewerberechtlichen Bestimmung des Zuverlässigkeitsbegriffs abweichen, ist keine datenschutzrechtliche Frage.

Der Gesetzentwurf knüpfte den Nachweis des Rechtsverstoßes nicht allein an eine rechtskräftige Verurteilung (§ 4 Abs. 2). Das ist angesichts der langen Dauer von Straf- und Ordnungswidrigkeitenverfahren in Wirtschaftssachen vertretbar. Ein zentraler Streitpunkt in der Diskussion über Korruptionsregister war und ist die Frage, ob und unter welchen Voraussetzungen ein Registereintrag bereits auf Verdachtsbasis erfolgen darf. Es ist anerkannt, dass die Unschuldsvermutung einem Registereintrag nicht entgegensteht, denn sie schützt nicht davor, bis zu einer rechtskräftigen Verurteilung keinerlei Nachteile erleiden zu müssen. Durch sie soll lediglich sichergestellt werden, dass Maßnahmen, die den vollen Nachweis der strafrechtlichen Schuld erfordern, erst getroffen werden dürfen, wenn dieser Nachweis tatsächlich erbracht worden ist. Eintragungen in das Korruptionsregister erfolgen jedoch schuldunabhängig. Daher können auch Verfahrenseinstellungen nach § 153a StPO an das Register gemeldet werden.

Mit den Benachrichtigungs-, Auskunfts-, Berichtigungs- und Löschungsregeln enthielt der Entwurf – unbeschadet der Rechtsschutzmöglichkeiten gegen unberechtigte Eintragungen – ausreichende verfahrensrechtliche Vorkehrungen, um zu verhindern, dass Registereintragungen, die bereits während eines Ermittlungsverfahrens erfolgen, zu einem unverhältnismäßigen Eingriff in die Rechte der Betroffenen führen würden.

3.1.2
Recht auf Akteneinsicht

Führt eine Behörde eine Akte mit Informationen zu einer Person, hat diese Person Anspruch auf Akteneinsicht. Dies habe ich in einem Fall sowohl gegenüber der Landeshauptstadt Wiesbaden als auch gegenüber dem Hessischen Umweltministerium deutlich gemacht. Das Recht auf Akteneinsicht umfasst auch das Recht auf Fertigung von Fotokopien.

Schon im vergangenen Tätigkeitsbericht hatte ich darüber berichtet, dass Bürger Schwierigkeiten hatten, Ihr Recht auf Akteneinsicht, das in § 18 Abs. 5 HDSG geregelt ist, gegenüber den Akten führenden Stellen durchzusetzen.

§ 18 Abs. 5 HDSG

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Ein Bürger hatte sowohl beim Umweltamt der Stadt Wiesbaden als auch beim Hessischen Umweltministerium Akteneinsicht beantragt, die ihm jedoch zunächst von beiden Stellen verwehrt wurde. Daraufhin wandte er sich an meine Dienststelle und bat um Unterstützung.

Zunächst galt es zu klären, ob dort tatsächlich Akten zur Person des Anfragenden geführt werden. Im Falle des Umweltamtes ist die Originalakte laut Erklärung des Amtes an die Obere Naturschutzbehörde abgegeben worden. Im Übrigen sei die Akte im Jahr 2009 und 2010 bereits der Rechtsanwältin des Antragstellers übersandt worden. Seit dieser Übersendung habe es keine neuen umweltrelevanten Sachverhalte gegeben. In einem Telefonat mit meiner Dienststelle erwähnte ein Mitarbeiter jedoch, dass es sehr wohl noch eine Akte zu dem Antragsteller gebe. Auf meine wiederholte Aufforderung hin, dem Antragsteller Akteneinsicht zu gewähren, hat das Amt die Akte letztlich an meine Dienststelle übersandt. Ich konnte feststellen, dass es sich ganz eindeutig um eine Akte im Sinne des § 18 Abs. 5 HDSG handelt.

Der Antragsteller hatte im Jahr 2010 gegenüber dem Umweltministerium eine fachaufsichtsrechtliche Überprüfung des Vorwurfs einer Ordnungswidrigkeit durch ein städtisches Amt beantragt und dazu einen 26-seitigen Schriftsatz an das Ministerium eingereicht. Da er auf diesen Antrag keine schriftliche Antwort erhielt, hat er durch seine Rechtsanwältin Akteneinsicht beantragt. Diese Akteneinsicht wurde ihm unter Hinweis darauf, dass es sich nicht um ein Verwaltungsverfahren nach § 29 HVwVfG handele, nicht gewährt. Deshalb wandte er sich an meine Dienststelle und bat um Unterstützung. Ich habe daraufhin das Umweltministerium angeschrieben und auf das Akteneinsichtsrecht nach § 18 Abs. 5 HDSG hingewiesen.

Das Ministerium teilte mir daraufhin mit, dass ein Grund für die fachaufsichtsrechtliche Überprüfung – wie vom Antragsteller begehrt – nicht vorlag. Dem Fachaufsichtbegehren lag ein Ordnungswidrigkeitenverfahren der Stadt Wiesbaden zugrunde, so dass mangels Zuständigkeiten beim Ministerium keinerlei Durchschriften gerichtlicher Verfügungen oder Schriftsätze der Beteiligten vorlagen. Insofern würde beim Ministerium auch keine Akte existieren, in die Einsicht gewährt werden könne.

Ich habe daraufhin das Umweltministerium aufgesucht und um Vorlage der vorhandenen Unterlagen zu dem Petenten gebeten. Dort wurde mir ein Ordner mit Schriftstücken vorgelegt, die alle mit der Antragstellung des Petenten zu tun hatten. Es handelte sich nach meinen Feststellungen eindeutig um eine Akte, die zu einer bestimmten Person geführt wurde, auch wenn der Name des Petenten nicht auf dem Aktenrücken stand. U. a. befand sich in dieser Akte eine rechtliche Stellungnahme zu der gewünschten Überprüfung des städtischen Amtes. Ich habe dem Ministerium deshalb mitgeteilt, dass dem Petenten ein Anspruch auf Akteneinsicht nach § 18 Abs. 5 HDSG zusteht.

Als ihm diese Einsicht im Hause des Ministeriums gewährt wurde, bat er darum, Kopien aus der Akte fertigen zu dürfen. Dies wurde ihm nicht gestattet, woraufhin er sich über seine Rechtsanwältin erneut mit der Bitte um Unterstützung an meine Behörde wandte. Ich habe daraufhin dem Umweltministerium mitgeteilt, dass nach meiner Auffassung das Recht auf Akteneinsicht nach § 18 Abs. 5 HDSG auch das Recht auf Fertigung von Abschriften bzw. Kopien umfasst. Auch wenn das HDSG dies nicht ausdrücklich regelt, so würde jedoch das mit der Gewährung der Akteneinsicht verfolgte Ziel, dass sich der Bürger gegebenenfalls auch juristisch über das in den Akten Niedergelegte auseinandersetzen kann, verfehlt, wenn keine Kopien gemacht werden könnten. Insofern ist die Fertigung einer Kopie die logische Konsequenz des Rechts auf Akteneinsicht.

Das Ministerium hat sich dieser Auffassung angeschlossen und dem Petenten die Überlassung von Kopien gegen Kostenerstattung zugesichert. Gleichzeitig hat das Ministerium angekündigt, dass auch für die bereits

gewährte Akteneinsicht eine entsprechende Gebühr in Rechnung zu stellen ist. Ich wurde daraufhin gebeten, auch die Rechtmäßigkeit der Gebührenforderung zu überprüfen.

Das Recht auf Akteneinsicht ergibt sich aus § 18 HDSG. In Abs. 3 der Vorschrift heißt es, dass dem Betroffenen gebührenfrei Auskunft zu erteilen ist. Abs. 5, der die Akteneinsicht regelt, nimmt Bezug auf Abs. 3, sodass die Gebührenfreiheit auch für die Akteneinsicht gilt. Im Übrigen stellt das Recht auf Akteneinsicht einen wesentlichen Bestandteil des Grundrechts auf informationelle Selbstbestimmung dar. Die Wahrnehmung dieses Grundrechts kann nicht von Geldleistungen abhängig gemacht werden. Insofern ist hier die Sachlage auch anders zu bewerten, als bei einer Akteneinsicht nach den Informationsfreiheitsgesetzen. Hier ist die Erhebung einer Gebühr durchaus rechtlich möglich. Allerdings setzt die Erhebung einer Gebühr auch dort eine Gebührenordnung voraus. Diese Rechtsauffassung habe ich dem Umweltministerium mitgeteilt, das sich dieser Auffassung angeschlossen hat.

3.2 Hessischer Landtag

3.2.1
Veröffentlichung von Besucherfotos im Internet und in Broschüren

Der Hessische Landtag darf Fotos, auf denen Besucher abgebildet sind, im Internet und in Druckwerken veröffentlichen.

Der Hessische Landtag verzeichnet jedes Jahr eine große Anzahl von Besuchern. Sie nehmen in Gruppen oder einzeln an Plenarsitzungen teil, sprechen mit Abgeordneten oder besichtigen das Schloss als Parlamentssitz. Für Jugendliche hält der Landtag besondere pädagogische Angebote bereit, die einen Einblick in die Arbeitsweise des Parlaments und Grundzüge des parlamentarischen Regierungssystems vermitteln sollen. Die Besuche werden regelmäßig durch Fotos dokumentiert. Dabei werden neben Gruppenfotos auch Einzelfotos angefertigt, die die Besucher in bestimmten Situationen, z. B. im Gespräch mit einem Abgeordneten, zeigen. Ausgewählte Fotos veröffentlicht der Landtag anschließend auf seiner Webseite oder in Druckerzeugnissen. Da die Veröffentlichung von Fotos von Privatpersonen rechtlich problematisch sein kann, bat mich der Landtag um Beratung.

3.2.1.1
Rechtslage nach dem KunstUrhG

Bildnisse dürfen gem. § 22 Satz 1 KunstUrhG grundsätzlich nur mit Einwilligung des Abgebildeten veröffentlicht werden. Sieht man in den Landtags-

besuchen öffentliche Veranstaltungen, könnte auf eine Einwilligung verzichtet werden, solange keine Porträtfotos angefertigt werden (§ 23 Abs. 1 Nr. 3 KunstUrhG).

Um das rechtliche Risiko zu minimieren, empfiehlt es sich jedoch, von der Notwendigkeit einer Einwilligung auszugehen. Eine Einwilligung nach KunstUrhG muss nicht schriftlich, sondern kann z. B. auch konkludent erfolgen. Es ist auch nicht erforderlich, dass der Betroffene geschäftsfähig ist. Bei Minderjährigen verlangt die herrschende Meinung eine Einwilligung des gesetzlichen Vertreters. Nach einer Mindermeinung ist allerdings auch die Einwilligung eines Minderjährigen wirksam, wenn er die Fähigkeit hat, die Bedeutung und Tragweite des Eingriffs in seine Persönlichkeitssphäre zu erkennen, das Für und Wider abzuwägen und seine Entscheidung nach dieser Einsicht zu bestimmen. Oberstufenschüler dürften über diese Fähigkeit verfügen. Lassen sich die Schüler wissentlich bei den Landtagsbesuchen fotografieren, könnte nach der Mindermeinung darin eine wirksame Einwilligung gesehen werden. Zu berücksichtigen ist auch, dass es sich bei den Fotos allenfalls um minimale Eingriffe in das Persönlichkeitsrecht der Schüler handelt, die nicht vergleichbar sind mit Aktfotos, Fotos von Straftaten oder Aufnahmen von Unfallopfern.

Geht man von der Notwendigkeit einer Einwilligung der Erziehungsberechtigten aus, wäre eine Widerspruchslösung als konkludente Einwilligung vertretbar. Um den bürokratischen Aufwand in akzeptablem Rahmen zu halten, habe ich dem Landtag folgendes Verfahren vorgeschlagen: Die Schule reicht über die Schüler ein Informationsblatt des Landtags an die Eltern weiter, in dem die Eltern über den Landtagsbesuch informiert werden, verbunden mit dem hervorgehobenen Hinweis, dass im Rahmen der Öffentlichkeitsarbeit des Landtags von dem Besuch Fotos angefertigt werden können und diese möglicherweise auf der Webseite des Landtags und in Druckerzeugnissen veröffentlicht werden. Den Eltern wird eine Widerspruchsmöglichkeit eingeräumt. Die Widerspruchserklärung könnten die Eltern über die Schüler an die Schule senden, die beim Besuch die Widerspruchserklärungen dem Landtag übergibt. Folgt man der Auffassung, dass auch Minderjährige wirksam einwilligen können, wären die Schüler allerdings nicht an den Widerspruch der Erziehungsberechtigten gebunden

Ein Widerruf der Einwilligung ist nach Kunsturheberrecht nur ausnahmsweise möglich. Der Widerruf einer Einwilligung zu einer Medienveröffentlichung ist nach der Rechtsprechung nur zulässig, wenn sich seit der erteilten Einwilligung die Umstände so gravierend geändert haben, das eine weitere Veröffentlichung das allgem. Persönlichkeitsrecht des Betroffenen verletzten würde.

Der Widerruf wirkt nur ex nunc. Daher genügt es, wenn das Bild von der Webseite des Landtags entfernt wird. Der Landtag ist nicht verpflichtet, dafür zu sorgen, dass das Bild auch aus dem Cache von Suchmaschinen oder auf gespiegelten Webseiten entfernt wird.

3.2.1.2
Rechtslage aufgrund des Hessischen Datenschutzgesetzes

Fraglich ist die Anwendbarkeit des Hessischen Datenschutzgesetzes. Es müsste sich bei dem Besucherdienst um eine Verwaltungsangelegenheit handeln (§ 39 Abs. 1 Satz 1 HDSG). Der Besucherdienst (Öffentlichkeitsarbeit, d.h. Vermittlung der Tätigkeit des Parlaments) dürfte allerdings der Legislative zuzuordnen sein, was insbesondere auch in der Teilnahme der Parlamentarier zum Ausdruck kommt. Das HDSG dürfte daher nicht anwendbar sein.

Wird die Anwendbarkeit des HDSG bejaht, stellt sich die Frage, ob eine Widerspruchslösung ausreichen könnte. Das Verfahren ist in Einzelfällen vertretbar, um einen unverhältnismäßigen bürokratischen Aufwand zu vermeiden. Angesichts des geringen Eingriffs, der mit der Aufnahme und Veröffentlichung der Fotos in Druckwerken oder auf der Webseite des Landtags verbunden ist, wäre dem Schutzbedürfnis der Betroffenen ausreichend gedient, wenn ihnen die Möglichkeit zum Widerspruch eingeräumt würde.

Hält man eine Einwilligung für nötig, müsste diese von den Schülern erklärt werden. Im Gegensatz zum Kunsturheberrecht ist im Datenschutzrecht unumstritten, dass auch Minderjährige in die Datenverarbeitung wirksam einwilligen können und müssen, wenn sie über die notwendige Einsichtsfähigkeit verfügen. Davon kann hier ausgegangen werden.

Vom Schriftformerfordernis bei der Einwilligung kann abgewichen werden, wenn wegen besonderer Umstände eine andere Form angemessen ist. Wenn die Schüler vorher durch ein Informationsblatt umfassend unterrichtet worden sind, dürfte eine mündliche Einwilligung der Betroffenen, die vom Fotografen kurz vor dem Fotografieren eingeholt wird, genügen.

Nach § 7 Abs. 2 Satz 6 HDSG kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden. Die Widerrufsmöglichkeit nach HDSG kollidiert mit der Rechtsprechung zum Widerruf der Einwilligung in die Veröffentlichung von Bildern nach Kunsturheberrecht. Der Landtag könnte jedoch auf das aus dem Kunsturheberrecht resultierende zivilrechtliche Abwehrrecht gegen den Widerruf verzichten. Der Widerruf hätte aber auch dann nur zur Folge, dass das Bild lediglich von der Webseite des Landtags

entfernt werden müsste. Aus bereits aufgelegten Druckwerken kommt eine Entfernung nicht in Betracht, sie müssen auch nicht eingestampft werden.

Der Landtag hat sich entsprechend meiner Empfehlung für das Widerspruchsverfahren entschieden.

3.3 Justiz und Polizei

3.3.1
Auskünfte zu Strafverfahren

Wiederholt hat es sich in diesem Jahr gezeigt, dass es in der Praxis immer wieder Schwierigkeiten gibt bei der Anwendung der Auskunftsregelungen der Strafprozessordnung.

3.3.1.1
Anfrage, ob es ein Ermittlungsverfahren gibt bzw. Bitte um Mitteilung eines Aktenzeichens

Ein Rechtsanwalt – der vermutete, dass gegen einen seiner Mandanten ein Ermittlungsverfahren geführt wurde – versuchte zu erfahren, unter welchem Aktenzeichen das Verfahren geführt würde. Dieses Auskunftsersuchen hat die Staatsanwaltschaft abgelehnt und sich dabei auf § 491 Abs. 1 S. 2 bis 4 StPO berufen.

Zur Verwaltung der Vorgänge bei der Staatsanwaltschaft wird ein automatisiertes Verfahren eingesetzt. Dieses enthält u. a. Daten zu den Personen, die in irgendeiner Rolle an einem Strafverfahren beteiligt sind, z. B. als Beschuldigter, Anzeigeerstatter, Zeuge, Opfer oder Verteidiger. Wiederholt hatten sich Bürger an mich gewandt, da ihnen nach ihrer Meinung zu Unrecht Auskunft zu laufenden Verfahren, etwa die Angabe eines Aktenzeichens, verweigert worden sei.

Ein Auskunftsanspruch aus der bei der Staatsanwaltschaft geführten Datei ergibt sich aus § 491 Abs. 1 StPO.

§ 491 Abs. 1 StPO

Dem Betroffenen ist, soweit die Erteilung oder Versagung von Auskünften in diesem Gesetz nicht besonders geregelt ist, entsprechend § 19 des Bundesdatenschutzgesetzes Auskunft zu erteilen. Auskunft über Verfahren, bei denen die Einleitung des Verfahrens bei der Staatsanwaltschaft im Zeitpunkt der Beantragung der Auskunft noch nicht mehr als sechs Monate zurückliegt, wird nicht erteilt. Die Staatsanwaltschaft kann die Frist des Satzes 2 auf bis zu 24 Monate verlängern, wenn wegen der Schwierigkeit oder des Umfangs der Ermittlungen im Einzelfall ein Geheimhaltungsbedürfnis fortbesteht. Über eine darüber

hinausgehende Verlängerung der Frist entscheidet der Generalstaatsanwalt, in Verfahren der Generalbundesanwaltschaft der Generalbundesanwalt. Die Entscheidungen nach den Sätzen 3 und 4 und die Gründe hierfür sind zu dokumentieren. Der Antragsteller ist unabhängig davon, ob Verfahren gegen ihn geführt werden oder nicht, auf die Regelung in den Sätzen 2 bis 5 hinzuweisen.

Für den Beschuldigten ist diese Norm im Regelfall daher nicht einschlägig, da das Einsichtsrecht in die Ermittlungsakten gem. § 147 StPO eine besondere Regelung enthält. Dieses Einsichtsrecht durch den Verteidiger gehört zu den Grundsätzen eines fairen Strafverfahrens.

§ 147 StPO

(1) Der Verteidiger ist befugt, die Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der Anklage vorzulegen wären, einzusehen sowie amtlich verwahrte Beweisstücke zu besichtigen.

(2) Ist der Abschluss der Ermittlungen noch nicht in den Akten vermerkt, kann dem Verteidiger die Einsicht in die Akten oder einzelne Aktenteile sowie die Besichtigung von amtlich verwahrten Beweisgegenständen versagt werden, soweit dies den Untersuchungszweck gefährden kann. Liegen die Voraussetzungen von Satz 1 vor und befindet sich der Beschuldigte in Untersuchungshaft oder ist diese im Fall der vorläufigen Festnahme beantragt, sind dem Verteidiger die für die Beurteilung der Rechtmäßigkeit der Freiheitsentziehung wesentlichen Informationen in geeigneter Weise zugänglich zu machen; in der Regel ist insoweit Akteneinsicht zu gewähren.

...

(7) Dem Beschuldigten, der keinen Verteidiger hat, sind auf seinen Antrag Auskünfte und Abschriften aus den Akten zu erteilen, soweit dies zu einer angemessenen Verteidigung erforderlich ist, der Untersuchungszweck, auch in einem anderen Strafverfahren, nicht gefährdet werden kann und nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Absatz 2 Satz 2 erster Halbsatz, Absatz 5 und § 477 Abs. 5 gelten entsprechend.

Zweck dieser Regelungen zur Auskunftsverweigerung ist das Verhindern von Ausforschungsversuchen. Aus verständlichen Gründen werden Ermittlungsverfahren zumindest teilweise bewusst so geführt, dass der Beschuldigte davon (noch) keine Kenntnis bekommt. Damit die Rechte der Betroffenen auch in diesem Stadium gewahrt werden, enthält die Strafprozessordnung eine Fülle von Regelungen zum Ausgleich dieser Heimlichkeit, wie z. B. die Notwendigkeit, dass bestimmte eingriffsintensive Ermittlungsmaßnahmen vom Richter angeordnet werden müssen. In einer Abwägung des Interesses des Staates an einer funktionierenden Strafrechtspflege mit den Anspruch des Betroffenen auf Kenntnis, wer Daten über ihn verarbeitet, hat der Gesetzgeber daher dieses gestufte Verfahren mit der zeitlich begrenzten Auskunftsverweigerung und den Verlängerungsmöglichkeiten geschaffen.

Auch für diese Fälle ist der Betroffene im Übrigen nicht schutzlos. Da § 491 Abs. 1 Satz 1 StPO für die Auskunft die entsprechende Anwendung des § 19 BDSG anordnet, ist die Auskunftsverweigerung durch den Datenschutzbeauftragten überprüfbar.

§ 19 BDSG

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. *die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,*
2. *die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und*
3. *den Zweck der Speicherung.*

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

...

(4) Die Auskunftserteilung unterbleibt, soweit

1. *die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,*
2. *die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder*
3. *die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen*

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

...

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

(7) Die Auskunft ist unentgeltlich.

Dabei ist zu beachten, dass die Staatsanwaltschaften Landesbehörden sind. Damit unterliegen diese meiner Kontrolle und nicht der des Bundesbeauftragten für den Datenschutz. Mit dem Verweis auf § 19 BDSG war keine Änderung in der Kontrollzuständigkeit beabsichtigt – dies wäre mangels Kompetenz des Bundesgesetzgebers auch nicht möglich gewesen.

Im geschilderten Fall hat meine Nachprüfung ergeben, dass die Staatsanwaltschaft berechtigt war, keine Auskunft zu erteilen.

3.3.1.2 Auskunftsersuchen des Betroffenen nach Abschluss des Strafverfahrens

Ein Bürger wandte sich an mich, da ihm die Kommune nach Abschluss eines Ordnungswidrigkeitenverfahrens Einsicht in die dortige Akte verweigerte. Das Verfahren war vom Amtsgericht durch Aufhebung des Bußgeldbescheides beendet worden.

Die Kommune stützte sich dabei auf § 147 StPO – der auch im Bußgeldverfahren zur Anwendung kommt – und verweigerte die Einsicht, da das Verfahren rechtskräftig beendet sei und weitere Verfahrenshandlungen nicht mehr möglich wären.

Der Bürger wollte die Einsicht in die Akte jedoch nicht, um das Bußgeldverfahren weiter zu betreiben. Er hatte die Vermutung, dass die Kommune im Rahmen des Bußgeldverfahrens nicht ordnungsgemäß gehandelt hatte. Deshalb wollte er prüfen, ob er ggf. weitere Ansprüche gegen die Kommune geltend machen könnte.

Aus diesem Grunde war ihm vollständige Einsicht in die Unterlagen zu gewähren, die bei der Kommune zur Durchführung des Ordnungswidrigkeitenverfahrens entstanden waren. Dies folgt aus § 475 StPO.

§ 475 StPO

(1) Für eine Privatperson und für sonstige Stellen kann, unbeschadet der Vorschrift des § 406e, ein Rechtsanwalt Auskünfte aus Akten erhalten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der öffentlichen Klage vorzulegen wären, soweit er hierfür ein berechtigtes Interesse darlegt. Auskünfte sind zu versagen, wenn der hiervon Betroffene ein schutzwürdiges Interesse an der Versagung hat.

(2) Unter den Voraussetzungen des Absatzes 1 kann Akteneinsicht gewährt werden, wenn die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern oder nach Darlegung dessen, der Akteneinsicht begehrt, zur Wahrnehmung des berechtigen Interesses nicht ausreichen würde.

Danach ist die verfahrensübergreifende Übermittlung von Daten aus Strafverfahren an solche Stellen oder Personen erlaubt, die nicht Verfahrensbeteiligte sind. Denn für diese gehen die speziellen Regelungen zu Auskunft bzw. Einsicht in die Akten vor, für den Beschuldigten etwa § 147 StPO. Nach einem abgeschlossenen Verfahren endet jedoch auch die Rolle der Verfahrensbeteiligten. Damit sind grundsätzlich alle Auskunftsersuchen nach

§ 475 StPO zu entscheiden. Eine Ausnahme gilt für den früheren Beschuldigten nur dann, wenn sein Auskunftsbegehren der Vorbereitung weiteren Prozesshandlungen in diesem Verfahren, wie etwa ein Wiederaufnahmeverfahren, dienen soll. Wird Akteneinsicht für Zwecke begehrt, die mit der Verteidigung des früheren Angeklagten in der Strafsache nicht mehr zusammen hängen, ist § 147 StPO nicht einschlägig.

Soll der Hintergrund eines Auskunftsersuchens allein dazu dienen, die fehlerhaften Handlungen der Verwaltung aufzudecken, stünde dies nicht mehr mit dem ursprünglichen Verfahren in Zusammenhang. Dann ist der Antragsteller wie jeder andere Dritte als „Privatperson“ im Sinne des § 475 StPO anzusehen.

Dann gilt auch für ihn, dass zu prüfen ist, ob er ein berechtigtes Interesse darlegt. Da es um die Akte eines gegen ihn geführten Verfahrens geht, kann auch kein schutzwürdiges Interesse des Betroffenen entgegenstehen.

3.3.1.3 Auskünfte an den Anzeigeerstatter

Wiederholt haben sich Bürger an mich gewandt, weil sie nicht erfahren haben, welche Konsequenzen sich aus von ihnen gestellten Anzeigen ergeben haben.

Gesetzlich vorgeschrieben ist eine Mitteilung an den Antragsteller dann, wenn die Staatsanwaltschaft kein Ermittlungsverfahren einleitet oder ein solches nach Abschluss der Ermittlungen einstellt.

§ 171 StPO

Gibt die Staatsanwaltschaft einem Antrag auf Erhebung der öffentlichen Klage keine Folge oder verfügt sie nach dem Abschluss der Ermittlungen die Einstellung des Verfahrens, so hat sie den Antragsteller unter Angabe der Gründe zu bescheiden. In dem Bescheid ist der Antragsteller, der zugleich der Verletzte ist, über die Möglichkeit der Anfechtung und die dafür vorgesehene Frist (§ 172 Abs. 1) zu belehren.

Diesem Bescheid ist auch eine Begründung beizufügen, aus der – in einer für den Antragsteller verständlichen Weise – hervorgeht, warum aus rechtlichen und/oder tatsächlichen Gründen keine Anklage erhoben wird.

Wird durch das Gericht die Anklage nicht zugelassen, wird darüber der Antragsteller ebenfalls in Kenntnis gesetzt.

§ 174 StPO

(1) Ergibt sich kein genügender Anlass zur Erhebung der öffentlichen Klage, so verwirft das Gericht den Antrag und setzt den Antragsteller, die Staatsanwaltschaft und den Beschuldigten von der Verwerfung in Kenntnis.

(2) Ist der Antrag verworfen, so kann die öffentliche Klage nur auf Grund neuer Tatsachen oder Beweismittel erhoben werden.

Über die Zulassung einer Anklage bzw. die Eröffnung des Hauptverfahrens wird ein Antragsteller jedoch nur in dem Fall unterrichtet, wenn er Nebenkläger ist.

Ist die Anklage zugelassen und das Hauptverfahren eröffnet, gibt es keine weiteren Mitteilungen. Die Hauptverhandlung einschließlich der Verkündung des Urteils ist öffentlich. Daher ging der Gesetzgeber davon aus, dass zusätzliche Informationen nicht notwendig sind. Die Transparenz des Strafverfahrens war ja damit gegeben.

Die aus Sicht des Rechts auf informationelle Selbstbestimmung notwendigen (ergänzenden) Regelungen wurden im Jahr 2000 in die StPO eingefügt. Als Folge dessen, kann eine Auskunft über ein Strafverfahren nunmehr auf Grundlage des § 475 StPO erfolgen. Dabei ist jeweils zu prüfen, ob ein berechtigtes Interesse besteht. Die Tatsache allein, das jemand eine Straftat angezeigt hat, wird in der Regel dafür nicht ausreichen.

Soweit ein Anzeigeerstatter oder auch ein Zeuge einer Straftat wissen möchte, ob bzw. welche Daten über ihn in diesem Zusammenhang bei der Staatsanwaltschaft gespeichert sind, erhält er diese Auskünfte auf Grundlage des § 495 StPO.

Einem Eingeber war eine solche Auskunft auf Mitteilung des Aktenzeichens zu den von ihm gestellten Strafanzeigen verwehrt worden. Dabei handelte es sich um eine Vielzahl von Anzeigen, die alle einen vergleichbaren Sachverhalt betrafen. Seine Mitgliedsrechte in einer Institution seien verletzt worden, die zuständigen internen Gremien würden ihrer Pflicht nicht nachkommen und gleichzeitig verweigere diese Institution ihm Auskünfte über die Ergebnisse seiner Beschwerden.

Meine Nachfragen bei der Staatsanwaltschaft ergaben, dass man den Sachverhalt sorgfältig überprüft habe, es aber keine Anhaltspunkte für ein strafbares Verhalten gäbe. Nach Rücksprache mit dem Justizministerium habe man daher nunmehr entschieden, zukünftig eingehende Schreiben zwar zu sichten, ihnen aber nur dann ein eigenes Aktenzeichen zuzuordnen, wenn im Zusammenhang mit einem neuen Sachverhalt sich Anhaltspunkte ergäben, die die Prüfung einer Einleitung eines Ermittlungsverfahrens not-

wendig machten. In allen anderen Fällen würden diese Schreiben in einer Sammelakte abgelegt. Eine Bescheidung des Eingebers würde nicht mehr erfolgen, da jede Mitteilung über die Ablehnung eines Ermittlungsverfahren dazu führe, dass eine Vielzahl neuer Schreiben eingingen, die keine neuen Anhaltspunkte lieferten.

Ich habe keine Bedenken gegen ein solches Vorgehen. Auch das Recht auf Auskunft im Rahmen des Rechts auf informationelle Selbstbestimmung hat insoweit Grenzen. Bei sogenannten uneinsichtigen Querulanten oder Kettenanzeigern, die einen erheblichen Arbeitsaufwand verursachen – ohne dass ihren Anschuldigungen eine Substanz zugrunde liegt, ist es gerechtfertigt, von einer Auskunft abzusehen. Der Eingriff in ihr Recht auf informationelle Selbstbestimmung ist hier gering, da die Behörde nur die Daten verarbeitet, die sie selbst der Behörde mitgeteilt haben.

3.3.2
Prüfung des Einsatzes der DNA-Analyse in der polizeilichen Praxis

Bei der Prüfung des Einsatzes der DNA-Analyse in der polizeilichen Praxis habe ich festgestellt, dass die Dokumentation der Voraussetzungen für eine solche Speicherung in den Akten in einigen Fällen sowohl formal als auch inhaltlich verbesserungswürdig ist.

In der Vergangenheit wurde ich mehrfach von Polizeibediensteten angesprochen, die Zweifel an der Praxis der hessischen Polizei bei der Speicherung von DNA-Daten hatten. Diese Anfragen haben mich dazu bewogen, mir im Rahmen einer Prüfung ein Bild von der Praxis des Einsatzes von DNA-Analysen zu machen. Rechtlicher Maßstab für meine Auswertung der Kriminalakten ist dabei § 81g Abs. 1 StPO.

§ 81g Abs. 1 StPO

Ist der Beschuldigte einer Straftat von erheblicher Bedeutung oder einer Straftat gegen die sexuelle Selbstbestimmung verdächtig, dürfen ihm zur Identitätsfeststellung in künftigen Straftaten Körperzellen entnommen und zur Feststellung des DNA-Identifizierungsmusters sowie des Geschlechts molekulargenetisch untersucht werden, wenn wegen der Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind. Die wiederholte Begehung sonstiger Straftaten kann dem Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichstehen.

Aufgrund der an mich herangetragenen Hinweise waren für mich bei der Prüfung solche Fälle von Interesse, bei denen die wiederholte Begehung sonstiger Straftaten zu einer Speicherung in der DNA-Analyse-Datei geführt hat. Von zwei verschiedenen Polizeipräsidien habe ich mir daher sämtliche

Kriminalakten vorlegen lassen, bei denen in einem bestimmten Zeitraum aus Anlass eines Diebstahls, eines Computerbetruges oder des Erschleichens von Leistungen eine Speicherung in der DNA-Analyse-Datei veranlasst wurde.

In formaler Hinsicht habe ich die mir vorgelegten Akten mit den polizeieigenen Vorgaben aus der Richtlinie zur DNA-Analyse/DNA-Analyse-Datei verglichen.

Während die Kriminalakten des einen von mir überprüften Polizeipräsidiums in formaler Hinsicht durchweg dieser Richtlinie und den darin vorgegebenen Formularen entsprach, war im Bereich des zweiten von mir geprüften Polizeipräsidiums in einer Reihe von Fällen zu bemängeln, dass die Unterlagen zur Analyse und Speicherung von DNA nur unvollständig oder gar nicht in den Akten aufzufinden waren.

Eine wesentliche inhaltliche Voraussetzung für die Entnahme von Körperzellen und die Speicherung der DNA-Daten in der DNA-Analyse-Datei ist, dass wie § 81g Abs. 1 StPO es fordert, eine Negativprognose erstellt wird. Erst wenn eine solche Negativprognose vorliegt, kann im nächsten Schritt die Entnahme der Körperzellen entweder mit Einwilligung des Betroffenen oder angeordnet durch einen richterlichen Beschluss erfolgen. Es ist also erforderlich, dass die Polizei eine entsprechende Negativprognose erstellt, bevor der Betroffene um eine Einwilligung zur Entnahme von Körperzellen gebeten wird. Bei meiner Prüfung musste ich jedoch feststellen, dass in der überwiegenden Anzahl der Fälle die Negativprognose erst im Nachgang zur Entnahme von Körperzellen dokumentiert wurde.

Die inhaltlichen Anforderungen an die Negativprognose sind nach der Rechtsprechung nicht allzu hoch anzusetzen. Allerdings fordert die Rechtsprechung, dass sich die Negativprognose auf zu erwartende Taten bezieht, bei deren Ermittlung die Speicherung der DNA von Nutzen sein kann. Eine Auseinandersetzung hiermit habe ich in einigen der Akten, bei denen z.B. wiederholte Ladendiebstähle und „Schwarzfahren“ zu einer Speicherung der DNA geführt hat, vermisst und für künftige Fälle angemahnt.

In den von mir untersuchten Fällen basierte die Entnahme der Körperzellen fast ausnahmslos auf einer schriftlichen Einwilligung der Betroffenen. Dieser Befund hat mich dazu veranlasst die Polizeipräsidien zu bitten, mir Vergleichszahlen zu nennen von solchen Fällen, in denen der Betroffene einer Entnahme von Körperzellen nicht zugestimmt hat und es deshalb zu keiner Speicherung in der DNA-Analyse-Datei gekommen ist. Nur durch einen Vergleich dieser Zahlen vermag ich zu beurteilen, ob man bei den vorliegenden Einwilligung davon ausgehen kann, dass diese tatsächlich freiwillig von den Betroffenen abgegeben wurden.

3.3.3
Elektronische Aufenthaltsüberwachung ehemaliger Straftäter

Wurde für Straftäter nach der Entlassung aus dem Straf- oder Maßregelvollzug die elektronische Aufenthaltsüberwachung als besondere Maßnahme der Führungsaufsicht angeordnet, übernimmt die in Hessen eingerichtete Gemeinsame Überwachungsstelle der Länder (GÜL) die Überwachung der Einhaltung dieser Anordnung. Die Erarbeitung der Konzeption und die Umsetzung wurden von mir begleitet.

Seit dem 1. Januar 2011 können Gerichte für Verurteilte, die nach ihrer Entlassung aus dem Straf- oder Maßregelvollzug unter Führungsaufsicht stehen, gemäß § 68b Abs. 1 Satz 1 Nr. 12 StGB eine elektronische Aufenthaltsüberwachung (EAÜ) anordnen.

Voraussetzung ist, dass das Anlassdelikt besonders schweren Straftaten, insbesondere dem Bereich der Sexualstraftaten, Gewaltstraftaten, Staatsschutzdelikten sowie Straftaten gegen die öffentliche Ordnung und gemeingefährlichen Straftaten zuzurechnen ist.

§ 68b Abs. 1 StGB

Das Gericht kann die verurteilte Person für die Dauer der Führungsaufsicht oder für eine kürzere Zeit anweisen,

1. *den Wohn- oder Aufenthaltsort oder einen bestimmten Bereich nicht ohne Erlaubnis der Aufsichtsstelle zu verlassen,*
2. *sich nicht an bestimmten Orten aufzuhalten, die ihr Gelegenheit oder Anreiz zu weiteren Straftaten bieten können,*
3. *zu der verletzten Person oder bestimmten Personen oder Personen einer bestimmten Gruppe, die ihr Gelegenheit oder Anreiz zu weiteren Straftaten bieten können, keinen Kontakt aufzunehmen, mit ihnen nicht zu verkehren, sie nicht zu beschäftigen, auszubilden oder zu beherbergen,*

...

12. *die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen.*

Das Gericht hat in seiner Weisung das verbotene oder verlangte Verhalten genau zu bestimmen. Eine Weisung nach Satz 1 Nummer 12 ist nur zulässig, wenn

1. *die Führungsaufsicht auf Grund der vollständigen Vollstreckung einer Freiheitsstrafe oder Gesamtfreiheitsstrafe von mindestens drei Jahren oder auf Grund einer erledigten Maßregel eingetreten ist,*
2. *die Freiheitsstrafe oder Gesamtfreiheitsstrafe oder die Unterbringung wegen einer oder mehrerer Straftaten der in § 66 Absatz 3 Satz 1 genannten Art verhängt oder angeordnet wurde,*
3. *die Gefahr besteht, dass die verurteilte Person weitere Straftaten der in § 66 Absatz 3 Satz 1 genannten Art begehen wird, und*

4. die Weisung erforderlich erscheint, um die verurteilte Person durch die Möglichkeit der Datenverwendung nach § 463a Absatz 4 Satz 2 der Strafprozessordnung, insbesondere durch die Überwachung der Erfüllung einer nach Satz 1 Nummer 1 oder 2 auferlegten Weisung, von der Begehung weiterer Straftaten der in § 66 Absatz 3 Satz 1 genannten Art abzuhalten.

Die Betroffenen müssen im Falle einer solchen Weisung die für eine elektronische Überwachung ihres Aufenthaltsort erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich führen und dürfen deren Funktionsfähigkeit nicht beeinträchtigen.

Nähere Einzelheiten zum Umgang mit den beim Einsatz der EAÜ entstehenden Daten werden in § 463a StPO festgelegt.

§ 463a Abs. 4 StPO

Die Aufsichtsstelle erhebt und speichert bei einer Weisung nach § 68b Absatz 1 Satz 1 Nummer 12 des Strafgesetzbuches mit Hilfe der von der verurteilten Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung; soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der verurteilten Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Die Daten dürfen ohne Einwilligung der betroffenen Person nur verwendet werden, soweit dies erforderlich ist für die folgenden Zwecke:

1. *zur Feststellung des Verstoßes gegen eine Weisung nach § 68b Absatz 1 Satz 1 Nummer 1, 2 oder 12 des Strafgesetzbuches,*
2. *zur Ergreifung von Maßnahmen der Führungsaufsicht, die sich an einen Verstoß gegen eine Weisung nach § 68b Absatz 1 Satz 1 Nummer 1, 2 oder 12 des Strafgesetzbuches anschließen können,*
3. *zur Ahndung eines Verstoßes gegen eine Weisung nach § 68b Absatz 1 Satz 1 Nummer 1, 2 oder 12 des Strafgesetzbuches,*
4. *zur Abwehr einer erheblichen gegenwärtigen Gefahr für das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung Dritter oder*
5. *zur Verfolgung einer Straftat der in § 66 Absatz 3 Satz 1 des Strafgesetzbuches genannten Art.*

Zur Einhaltung der Zweckbindung nach Satz 2 hat die Verarbeitung der Daten zur Feststellung von Verstößen nach Satz 2 Nummer 1 in Verbindung mit § 68b Absatz 1 Satz 1 Nummer 1 oder 2 des Strafgesetzbuches automatisiert zu erfolgen und sind die Daten gegen unbefugte Kenntnisnahme besonders zu sichern. Die Aufsichtsstelle kann die Erhebung und Verarbeitung der Daten durch die Behörden und Beamten des Polizeidienstes vornehmen lassen; diese sind verpflichtet, dem Ersuchen der Aufsichtsstelle zu genügen. Die in Satz 1 genannten Daten sind spätestens zwei Monate nach ihrer Erhebung zu löschen, soweit sie nicht für die in Satz 2 genannten Zwecke verwendet werden. Bei jedem Abruf der Daten sind zumindest der Zeitpunkt, die abgerufenen Daten und der Bearbeiter zu protokollieren; § 488 Absatz 3 Satz 5 gilt entsprechend. Werden innerhalb der Wohnung der verurteilten Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verwertet werden und sind unverzüglich nach Kenntnisnahme zu löschen. Die Tatsache ihrer Kenntnisnahme und Löschung ist zu dokumentieren.

Die StPO schreibt bewusst keine bestimmte Technik zur Umsetzung der EAÜ vor. Der Einsatz von Geräten mit „GPS-Ortung“ zur jederzeitigen Feststellung des Aufenthaltsortes ist damit zulässig.

Die dabei anfallenden Bewegungsdaten dürfen jedoch nicht zur Erstellung eines laufenden Bewegungsprofils genutzt werden. Eine Kenntnisnahme soll – punktuell – jeweils nur dann erfolgen, wenn die besonderen Voraussetzungen zur Verwendung dieser Daten vorliegen. Darauf wird in der Begründung zum Gesetzentwurf (BTDrucks. 17/3403, S. 76) explizit hingewiesen. Deshalb ist auch ausdrücklich die automatisierte Verarbeitung dieser Daten angeordnet. Die Festlegungen des Gesetzgebers sind bei der technischen und organisatorischen Ausgestaltung der Umsetzung der gesetzlichen Vorgaben zu beachten.

Nicht in allen Fällen, in denen ein Richter eine Weisung gem. § 68b StGB anordnet, wird der Einsatz eines solchen Systems zur „GPS-Ortung“ sinnvoll möglich sein. So ist z. B. eine Auflage, sich nicht Orten zu nähern bzw. dort aufzuhalten, an denen sich Kinder befinden, mit dieser Technik in der Praxis so gut wie nicht kontrollierbar. Die Anzahl von Spielplätzen, Kindergärten etc. ist so groß, dass ggf. kein Raum bleibt, an dem der Proband sich aufhalten könnte. Damit könnte er seinen Alltag vom Einkaufen bis zum Arztbesuch oft gar nicht gestalten, ohne dass er Alarmmeldungen auslöst.

Wie häufig diese Maßnahme von Richtern angeordnet werden wird, lässt sich nicht voraussehen. Unabhängig davon ist es erforderlich, die notwendige technische Infrastruktur vorzuhalten. Der Aufwand ist recht groß. Unter anderem wird eine 24-Stunden-Bereitschaft zur Überwachung der Monitore notwendig. Eine solche kann nicht erst aufgebaut werden, wenn eine entsprechende Anordnung ergangen ist. Deshalb haben sich die Länder entschlossen, dies gemeinschaftlich durchzuführen. Ausgehend von den langjährigen Erfahrungen mit dem Einsatz von Fußfesseln werden wesentliche Teile der Konzeption in Hessen für alle verwirklicht. Dazu wurde ein Staatsvertrag geschlossen. Die Details der Umsetzung wurden zusätzlich in einer Verwaltungsvereinbarung geregelt.

Dabei liegt folgendes Konzept zugrunde:

Es wird eine gemeinsame Überwachungsstelle der Länder (GÜL) gegründet. Der GÜL werden durch den Staatsvertrag ein Teil der Aufgaben der Führungsaufsichtstelle übertragen. Dazu gehören die Entgegennahme und Bewertung von Alarmmeldungen sowie die Ursachenermittlung. Soweit erforderlich unterrichtet sie die Polizei bei Weisungsverstößen. Die GÜL ist eine hessische öffentliche Stelle und unterliegt daher meiner datenschutzrechtlichen Kontrolle für alle Daten, die sie verarbeitet.

Zur Erfüllung ihrer Aufgabe übermittelt die jeweilige Führungsaufsichtstelle für den Probanden, der die Fußfessel tragen soll, die erforderlichen persönlichen Daten. Dies sind neben den Angaben zu Person, Wohnort und telefonischer Erreichbarkeit insbesondere die Angaben zu den Orten, an denen der Betreffende sich auf Grundlage einer richterlichen Weisung nicht aufhalten darf. Zusätzlich erhält sie Daten über die zugrundeliegende Tat und ggf. weitere Informationen zur Person des Probanden. Dies benötigt die GÜL, um im Falle einer Alarmmeldung zu entscheiden, welche Reaktion zu erfolgen hat, bzw. wer zu informieren ist. (Genügt eine telefonische Ansprache des Betroffenen oder ist die Führungsaufsichtstelle zu informieren? Muss die Information sofort erfolgen oder kann bis zum nächsten Tag abgewartet werden? Ist eine zusätzliche Meldung an die Polizei notwendig?)

In der Datenbank, die zum System der EAÜ gehört, sind – neben den Angaben zu den Bereichen, die ein Proband nicht betreten soll, sowie den Kontaktdaten der Personen, die ggf. zu informieren sind – nur pseudonymisierte Daten der Probanden gespeichert. Die weiteren Daten, die die GÜL zu den einzelnen Personen benötigt, werden in einer getrennten Datenbank verarbeitet. Eine strikte Trennung der Daten wird dadurch erreicht, dass die EAÜ in einem eigenen physikalischen Netz läuft.

Die technische Betreuung für das System der elektronischen Aufenthaltsüberwachung übernimmt im Auftrag der GÜL die HZD als IT-Dienstleisterin für die hessische Landesverwaltung mit den Standorten in Wiesbaden und Hünfeld. Am Standort Hünfeld wurde dazu ein Technisches Monitoring Center eingerichtet, welches ebenfalls im Schichtbetrieb 24 Stunden am Tag und sieben Tage die Woche Dienst leistet. Das Technische Monitoring Center leistet die Betreuung des Systems, etwa das Anlegen der Probanden im System, die Eintragung von Einschluss- oder Ausschluss-Zonen, die Bearbeitung technischer Fehlermeldungen und die Weiterleitung der anderen Fehlermeldungen an die GÜL. Das Verfahrensmanagement, das ebenfalls bei der HZD angesiedelt ist und personell vom TMC getrennt ist, hat weitere Aufgaben wie das Anlegen von Nutzern und Auswertungen.

Um den ordnungsgemäßen Umgang mit den sehr sensiblen Daten sicherzustellen, ist es notwendig, sehr sorgfältig zu definieren, wer zu welchem Zeitpunkt Zugriff auf diese Daten bekommen darf. Dazu dient das Berechtigungskonzept, das differenziert zwischen den technischen Zugriffen im Rahmen der Verfahrensbetreuung und denen der Überwachungspersonen.

Auch im kommenden Jahr werde ich die Umsetzung der gesetzlichen Anforderungen weiter beobachten.

3.4 Ausländerwesen

3.4.1
EuGH-Urteil zur Nutzung des Ausländerzentralregisters – Umsetzung in der polizeilichen Praxis

Mit einem Urteil aus dem Jahr 2008 hat der Europäische Gerichtshof die Möglichkeiten der Verarbeitung von Daten von Unionsbürgern, die im Ausländerzentralregister gespeichert werden, erheblich eingeschränkt und insbesondere die Verarbeitung dieser Daten zum Zwecke der Kriminalitätsbekämpfung für unzulässig erklärt. Aufgrund der unzureichenden Reaktion des Bundesgesetzgebers auf das Urteil habe ich mich mit der praktischen Umsetzung des Urteils im Bereich der Polizei befasst.

Mit dem Urteil des EuGH vom 16. Dezember 2008 (C-524/06) wurde festgestellt, dass die Nutzung der im Ausländerzentralregister (AZR) gespeicherten Daten ausländischer Unionsbürger zur Kriminalitätsbekämpfung mit dem Diskriminierungsverbot von Unionsbürgern nicht vereinbar und daher unzulässig ist. Eine wesentliche Aussage des Urteils ist, dass die Daten von Unionsbürgern, die in diesem Register gespeichert sind, nur noch für aufenthaltsrechtliche Zwecke und in anonymisierter Form zu statistischen Zwecken verarbeitet werden dürfen.

Zur Anpassung der deutschen Rechtslage an die Forderungen des Urteils des Europäischen Gerichtshofs hat die Bundesregierung in einem ersten Schritt die Allgemeine Verwaltungsvorschrift zum Gesetz über das Ausländerzentralregister und zur Verordnung zur Durchführung des Gesetzes über das Ausländerzentralregister geändert. Im Wesentlichen wurde die Verordnung dabei lediglich um den Hinweis ergänzt, dass bei Abrufen von Daten ausländischer Unionsbürger die Maßgaben des Urteils zu beachten sind und ein Zugriff auf die Daten allein zum Zwecke der Kriminalitätsbekämpfung unzulässig ist.

Da die Formulierungen in der Allgemeinen Verwaltungsvorschrift keinerlei konkrete Handlungsanweisungen für die betroffenen Stellen wie z. B. die Polizei enthält, habe ich mich bei dem Hessischen Landeskriminalamt erkundigt, wie die Forderungen des Europäischen Gerichtshofes dort praktisch umgesetzt werden.

Eine Umfrage in den verschiedenen Abteilungen des Hessischen Landeskriminalamts hat ergeben, dass das Urteil des EuGH in den einzelnen Fachabteilungen allgemein bekannt war und weitgehend auch umgesetzt wurde. In einzelnen Bereichen bestanden jedoch noch Unsicherheiten darüber, wie die Formulierung des EuGH, die Verarbeitung der AZR-Daten von Uni-

onsbürgern *„zum Zwecke der Kriminalitätsbekämpfung“* sei unzulässig, zu interpretieren sei. So wurde etwa die Auffassung vertreten, mit *„Kriminalitätsbekämpfung“* sei nur Strafverfolgung gemeint und eine Nutzung der Daten zum Zwecke der Abwehr künftiger Gefahren sei weiterhin zulässig. Auf meine Empfehlung wurde daher ein Rundschreiben verfasst, in dem noch einmal klargestellt wurde, dass auf Grund des Urteils weder aus Gesichtspunkten der Strafverfolgung noch aus Gründen der Gefahrenabwehr eine AZR-Abfrage in Bezug auf Unionsbürger zulässig ist.

Hieraus folgt für die Arbeit der Polizei, dass – sofern konkrete Anhaltspunkte bestehen, dass es sich bei betroffenen Personen um EU-Bürger handelt – die Abfrage des AZR im Rahmen von Ermittlungen oder der täglichen polizeilichen Arbeit generell zu unterbleiben hat. Erlangt die Polizei erst bei der Abfrage des AZR Kenntnis davon, dass es sich um einen Unionsbürger handelt, ist die Abfrage unverzüglich abzubrechen und die durch die unzulässige Abfrage gewonnenen Erkenntnisse dürfen für die weiteren Ermittlungen und folgende polizeiliche Arbeit nicht genutzt und müssen gegebenenfalls auch aus den Akten entfernt werden. Der Zugriff auf die Daten bleibt danach allein in solchen Fällen möglich, in denen es um die Umsetzung aufenthaltsrechtlicher Vorschriften geht.

Ich strebe an, beim HMDIS einen vergleichbaren Erlass anzuregen, damit auch in den Polizeipräsidien eine einheitliche Umsetzung aus den Forderungen des Urteils des EuGH erfolgt.

Inzwischen liegt ein Referentenentwurf zur Änderung des Ausländerzentralregistergesetzes vor, mit dem auch die Gesetzeslage an das Urteil des EuGH angepasst werden soll. Dieser soll noch im November 2011 vom Kabinett behandelt werden, um ein Vertragsverletzungsverfahren der Europäischen Kommission abzuwenden.

Durch die im Entwurf vorgesehenen Regelungen wird die Menge der zu Unionsbürgern im AZR zu speichernden Daten reduziert und z. B. auf die Speicherung eines Lichtbildes verzichtet. Darüber hinaus wird klargestellt, dass entsprechend der Feststellungen des EuGH die Verarbeitung dieser Unionsbürgerdaten nur zu ausländer- oder asylrechtlichen Zwecken zulässig ist. Eine Übermittlung dieser Daten kommt daher auch nur noch an solche Behörden in Betracht, die mit ausländer- oder asylrechtlichen Aufgaben betraut sind. Eine Liste der Behörden, die hierfür infrage kommen, enthält der Entwurf leider nicht.

3.4.2
Visawarndatei und Abgleich am Visumverfahren beteiligter Personen mit der Antiterrordatei

Die Bundesregierung hat ein Gesetz zur Errichtung einer Visawarndatei und zur Änderung aufenthaltsrechtlicher Vorschriften vorgelegt. Zu dem im Aufenthaltsgesetz geplanten Abgleich von Daten aller am Visumverfahren beteiligter Personen mit der Antiterrordatei habe ich mich kritisch geäußert.

In der im Entwurf der Bundesregierung zur Errichtung einer Visawarndatei und zur Änderung des Aufenthaltsgesetzes (BTDrucks. 17/6643 vom 20. Juli 2011) vorgelegten Visawarndatei sollen Daten von Personen, die bestimmte Straftaten begangen haben, sowie von jenen, die als Antragsteller oder Einlader falsche Angaben gemacht haben oder von Personen, die einer Verpflichtung zur Kostenübernahme für die Eingeladenen nicht nachgekommen sind, in einer zentralen Datei gespeichert werden, die vom Bundesverwaltungsamt geführt wird. Die nunmehr geplante Regelung weist gegenüber früheren Entwürfen aus datenschutzrechtlicher Sicht Verbesserungen auf. Betroffen sind nicht mehr alle am Visumverfahren beteiligten Personen, sondern nur solche, die bereits mit bestimmten, der Rechtsordnung widersprechenden Verhaltensweisen im Visumverfahren oder mit rechtskräftigen Verurteilungen wegen bestimmter Straftaten mit Bezug zum Visumverfahren aufgefallen sind. Positiv zu bewerten ist auch, dass der Zugriff auf die zentrale Datei auf Behörden beschränkt ist, die in das Visumserteilungsverfahren eingebunden sind. Anders als in früheren Entwürfen ist ein Zugriff von Sicherheitsbehörden und Nachrichtendiensten nicht mehr vorgesehen.

Aus datenschutzrechtlicher Sicht kritisch zu sehen ist der durch eine Änderung des Aufenthaltsgesetzes vorgesehene Abgleich sämtlicher Daten aller im Visumverfahren beteiligter Personen mit dem Datenbestand der Antiterrordatei beim Bundeskriminalamt. Nach dem geplanten § 72a AufenthG sollen Daten zur Visum antragstellenden Person, zum Einlader, zu Personen, die durch Abgabe einer Verpflichtungserklärung oder in anderer Weise die Sicherung des Lebensunterhalts gewähren und zu den sonstigen Referenzpersonen an das Bundesverwaltungsamt übermittelt werden. Bei einer dort angesiedelten besonderen Organisationseinheit soll ein Abgleich mit Daten aus der Antiterrordatei zu Personen erfolgen, bei denen Verdacht auf terroristische Aktivitäten besteht. Im Trefferfall wird die Behörde benachrichtigt, die die Daten in die Antiterrordatei eingegeben hat. Diese Behörde übermittelt der für das Visumverfahren zuständigen Auslandsvertretung über das Bundesverwaltungsamt einen Hinweis, wenn Gründe für die Versagung des Visums oder sonstige Sicherheitsbedenken gegen die Visumserteilung

bestehen. Kritisch angemerkt habe ich in meiner Stellungnahme, dass die Daten sämtlicher am Visumverfahren beteiligten Personen an das Bundesverwaltungsamt übermittelt werden, ohne dass Anhaltspunkte für ein pflichtwidriges Verhalten bestehen. Die Erforderlichkeit dieses Verfahrens, durch das überwiegend Personen betroffen werden, die sich rechtmäßig verhalten und keinen Anlass für eine Überprüfung gegeben haben, ist nicht dargetan.

Zweifel an der Erforderlichkeit drängen sich insbesondere dadurch auf, dass für Visumantragsteller aus bestimmten, als „kritisch“ eingestuften Herkunftsstaaten bereits das Konsultationsverfahren nach § 73 AufenthG existiert.

§ 73 AufenthG

(1) Die im Visumverfahren von der deutschen Auslandsvertretung erhobenen Daten der visumantragstellenden Person und des Einladers können über das Auswärtige Amt zur Feststellung von Versagungsgründen nach § 5 Abs. 4 an den Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz, den Militärischen Abschirmdienst, das Bundeskriminalamt und das Zollkriminalamt übermittelt werden. ...

...

(4) Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Auswärtigen Amt und unter Berücksichtigung der aktuellen Sicherheitslage durch allgemeine Verwaltungsvorschrift, in welchen Fällen gegenüber Staatsangehörigen bestimmter Staaten sowie Angehörigen von in sonstiger Weise bestimmten Personengruppen von der Ermächtigung des Abs. 1 Gebrauch gemacht wird.

An keiner Stelle des Entwurfs wird ausgeführt, warum sich das bisherige Konsultationsverfahren (mit der Flexibilität der durch Verwaltungsvorschrift zu verändernden Liste der als kritisch eingestuften Länder) nicht als ausreichend erwiesen hat.

3.4.3 Sicherheitsbefragungen im Rahmen der Erteilung von Aufenthaltstiteln

Das Recht auf Akteneinsicht in das Protokoll von Sicherheitsbefragungen im Rahmen von Aufenthaltstiteln soll in einem Erlass des Hessischen Ministeriums des Innern und für Sport klargestellt werden. Eine Verweigerung des Akteneinsichtsrechts kommt nur in eng begrenzten Ausnahmefällen in Betracht.

Im 39. Tätigkeitsbericht (Ziff. 4.4.2) habe ich über Probleme bei der Akteneinsicht von ausländischen Bürgerinnen und Bürgern bzw. deren Anwälten

in die Protokolle der Sicherheitsbefragungen im Rahmen der Erteilung von Aufenthaltstiteln berichtet. Im Berichtszeitraum wurde anlässlich der bundesrechtlich vorgeschriebenen Änderung der Beteiligung von Sicherheitsbehörden im Aufenthaltsverfahren auch das Verfahren der Sicherheitsbefragungen geändert. Derartige Befragungen ausländischer Bürger erfolgen immer dann, wenn den im Aufenthaltsverfahren beteiligten Sicherheitsbehörden, d. h. dem Hessischen Landesamt für Verfassungsschutz (HLfV), dem Landeskriminalamt (LKA) sowie den Nachrichtendiensten des Bundes sog. sicherheitsrelevante Erkenntnisse über die Betroffenen vorliegen. Derartige sicherheitsrelevante Erkenntnisse sind in § 54 Nr. 5 bis 5b AufenthG genannt.

§ 54 AufenthG

Ein Ausländer wird in der Regel ausgewiesen, wenn

…

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

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

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

Nach der neuen Rechtslage sollen diese Befragungen nicht mehr von der zuständigen Ausländerbehörde, sondern von den für das Ausländerrecht zuständigen Dezernaten der Regierungspräsidien durchgeführt werden. Erreicht werden soll damit eine Qualitätsverbesserung und eine Vereinheitlichung der Befragungen. Für diese Befragung werden zum Teil Formulare benutzt, die aber individuell verändert werden können.

In einem Erlass des HMDIS soll jetzt klar gestellt werden, dass der ausländische Bürger vor der Befragung belehrt werden muss, insbesondere ist er auf die Rechtsfolgen falscher oder unvollständiger Angaben hinzuweisen. Eine derartige Rechtsfolge kann beispielsweise die Ausweisung aus dem Bundesgebiet darstellen. Weiterhin ist klargestellt, dass der Betroffene das Recht hat, einen Dolmetscher bei der Befragung hinzuzuziehen.

Eine weitere wichtige Klarstellung besteht darin, dass festgehalten wird, dass der ausländische Bürger bzw. sein Anwalt das Recht besitzt, in die Protokolle über die Befragungen Einsicht zu nehmen. Eine Verweigerung der Akteneinsicht kann nicht auf § 29 Abs. 1 Satz 2 HVwVfG gestützt werden.

§ 29 Abs. 1 HVwVfG

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.

Wichtig ist, dass das Protokoll über eine Sicherheitsbefragung keinen Entwurf für eine Entscheidung im Sinne von Satz 2 darstellt.

Die Voraussetzungen einer Verweigerung der Akteneinsicht nach § 29 Abs. 2 HVwVfG dürften in den seltensten Fällen gegeben sein.

§ 29 Abs. 2 HVwVfG

Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit durch sie die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt, dass Bekanntwerden des Inhalts der Akten dem Wohle des Bundes oder eines Landes Nachteile bereiten würde. …

Da das Protokoll eine Zusammenstellung der mit dem Betroffenen besprochenen Fragen darstellt, kann es regelmäßig keine Inhalte aufweisen, die dem Betroffenen nicht bereits bekannt sind.

3.5 Verkehr

3.5.1
E-Ticket des RMV

Seit November 2011 werden im Gebiet des RMV Jahreskarten nur noch als Chipkarten ausgegeben. Damit wird ein erster Schritt unternommen, um eine E-Ticket-Infrastruktur einzurichten.

Seit vielen Jahren gibt es Planungen und immer wieder Pilotprojekte, in denen versucht wird, den Papierfahrschein durch neue, elektronische Varianten zu ergänzen oder sogar zu ersetzen. Beim 5. Europäischen Datenschutztag im Januar 2011 hatte ich über das Projekt Handy-Ticket des RMV berichtet. Dieses läuft weiter, wird jedoch auf Bundesebene durch weitere Varianten wie das Handy-Ticket Deutschland oder das Touch &Travel-Ticket ergänzt. Ein neuer elektronischer Fahrschein wurde dieses Jahr im Gebiet des RMV eingeführt: die Chipkarte als Ersatz für die Jahreskarte.

Basis dieser Form des Fahrscheins ist die sogenannte VDV-Kernapplikation. Dabei handelt es sich um eine IT-Anwendung mit zentralen Komponenten, Lesegeräten und einer Chipkarte, auf der der Fahrschein gespeichert wird. Der Verband Deutscher Verkehrsunternehmen (VDV) hat die Anforderungen an ein derartiges System festgeschrieben, damit es überall in Deutschland gleich funktioniert und, in der Endausbaustufe, eine einzige Chipkarte überall in Deutschland als Fahrschein im Öffentlichen Personennahverkehr (ÖPNV) genutzt werden kann. Auf dem Weg dorthin wurden Ausbaustufen definiert, von denen der Rhein-Main-Verkehrsverbund (RMV) mit seiner Chipkarte als Zeitkarte die Stufe 2 umsetzt.

Stufe 1: Bargeldlos bezahlen

Diese Stufe ist als ein Schritt auf die anderen Varianten zu sehen und wird beim RMV nicht gegangen.

Stufe 2: Elektronischer Fahrschein (EFS)

Hier bietet der RMV eine Teilmenge der möglichen Fahrscheine, die Zeitkarten, an. Zu Anfang werden die Jahreskarten umgestellt.

Stufe 3a: Check-In/Check-Out (CICO)

Bei dieser Technik muss man beim Betreten bzw. Verlassen des Fahrzeugs ein Lesegerät bedienen. Es wird dabei auf der Chipkarte ein Fahrschein erzeugt und in den Lesegeräten der Lesevorgang gespeichert. Zu Abrechnungszwecken werden in einem Hintergrundsystem aus den Datensätzen der Lesegeräte die Fahrten gebildet und gespeichert.

Stufe 3b: Be-In/Be-Out (BIBO)

Bei dieser Technik werden zwischen den Haltestellen durch Lesegeräte alle im Fahrzeug befindlichen Karten gelesen und wie bei der Stufe 3a auf der Chipkarte und in den Lesegeräten Datensätze gespeichert. Aus den Datensätzen der Lesegeräte werden wiederum im Hintergrundsystem die Fahrten gebildet und abgerechnet.

Da es bei Zeitkarten keine Abrechnung nach Fahrten gibt, werden in den Hintergrundsystemen keine Daten über einzelne Fahrten gespeichert. Insofern gibt es einen erheblichen Unterschied zu den Varianten, bei denen einzelne Fahrten zu Abrechnungszwecken gespeichert und für längere Zeit vorgehalten werden.

Die eingeführte Chipkarte nutzt eine RFID-Technik auf Basis der Normenreihe ISO 14443. Sie kann nur aus Entfernungen von wenigen Zentimetern ausgelesen werden und ist daher für die Stufe 3b (BIBO) so nicht nutzbar. In der jetzigen Ausbaustufe sind noch keine Lesegeräte in den Bussen und Bahnen installiert, da sie bei Zeitkarten nicht benötigt werden. Kontrolleure haben jedoch Kontrollterminals, das sind Lesegeräte, mit denen sie die Chipkarten auslesen können. Vor dem Zugriff auf die Daten wird durch die Chipkarte geprüft, ob es sich um ein zugelassenes Lesegerät handelt.

Abläufe
Als normaler Vertriebsweg werden die Kunden registriert und erhalten dann die Chipkarte mit der gespeicherten Jahreskarte. Da alle Jahreskarten nur noch als Chipkarte ausgegeben werden, also ein Nutzungszwang besteht, muss es auch eine anonym zu nutzende Variante geben. Diese Möglichkeit ist vom RMV vorgesehen. Man kann ohne Angabe persönlicher Daten eine Chipkarte erhalten, auf die dann eine Jahreskarte und zukünftig auch eine Monatskarte oder Wochenkarte aufgeladen werden kann. Soweit man mit Bargeld zahlt, gibt es keine Möglichkeit für den RMV, auf den Fahrgast zu schließen.

Verlust
Wenn man seine Karte verliert, kann man den Verlust melden und erhält einen Ersatz. Dies ist auch in der anonymen Variante möglich; dazu muss man unter Vorlage des Kaufbeleges nachweisen, dass man diese Chipkarte erworben hat. Die Kartennummern der als verloren gemeldeten Karten werden vom RMV im Hintergrundsystem gespeichert. Jeden Tag wird die Datei auf die Kontrollterminals geladen.

Kontrolle
Bei Kontrollen prüft der Kontrolleur mit seinem Lesegerät, ob die Karte gültig ist. Dazu muss die gespeicherte Zeitkarte zeitlich gültig sein und die Karte darf nicht als gestohlen gemeldet sein.

Rückgabe
Bei der Rückgabe werden Guthaben zurück überwiesen. Im Fall der anonymen Nutzung muss auch hier der Kaufbeleg vorgezeigt werden, bevor ein Guthaben ausgezahlt wird.

3.6 Schulen, Schulverwaltung und Hochschulen

3.6.1
Rechtsänderungen im Schulbereich

Im Berichtsjahr kam es zu einigen Rechtsänderungen im Schulbereich. Die Novellen waren aus datenschutzrechtlicher Sicht wenig relevant, aber nicht völlig unstrittig. Das Kultusministerium hat mir jeweils Gelegenheit gegeben, zu den vorgesehenen Rechtsvorschriften Stellung zu nehmen. Davon habe ich Gebrauch gemacht.

3.6.1.1
Lehrerbildungsgesetz

Das Lehrerbildungsgesetz enthält – wie die Vorgängerfassung – nur sehr wenige bereichsspezifische datenschutzrechtliche Regelungen. Es findet daher bei der Lehrerbildung nahezu uneingeschränkt das Hessische Datenschutzgesetz Anwendung. Es war nichts dagegen einzuwenden, dass es dabei bleibt. Das neue Hessische Lehrerbildungsgesetz ist am 28. Oktober 2011 in Kraft getreten.

3.6.1.2
Verordnung zur Umsetzung des Lehrerbildungsgesetzes

Die Verordnung präzisiert im Sinne des Datenschutzrechts hinreichend die Erforderlichkeit der personenbezogenen Datenverarbeitung bei der Lehrerausbildung. Insoweit war die Verordnung zu begrüßen.

An einer Stelle allerdings habe ich formelle wie inhaltliche Einwände gemacht: Im Gegensatz zur Juristenausbildung (dort in § 54 Abs. 1 Nr. 5 JAG) oder bei der allgemeinen Hochschulausbildung (dort in § 20 Abs. 2 Nr. 13 Hessisches Hochschulgesetz) enthalten die Ermächtigungen in §§ 34 und 54 des Lehrerbildungsgesetzes, die nähere Ausgestaltung der Staatsprüfungen mittels Rechtsverordnung zu regeln, keine ausdrückliche Bezeichnung einer Regelungsermächtigung zum Recht auf Einsicht in die Prüfungsunterlagen nach abgeschlossener Prüfung. Ich halte daher eine Regelungsbefugnis mittels Rechtsverordnung für nicht gegeben.

Davon unabhängig hielt ich eine in § 22 Abs. 3 des Verordnungsentwurfes vorgesehene Regelung, das Recht nur einmal zu gewähren, sowie eine weitere vorgesehene Beschränkung in § 22 Abs. 4 des Verordnungsentwurfes, dem Bewerber gegen Kostenerstattung Kopien der Prüfungsakte ausschließlich im Falle des Widerspruches anzufertigen, für unverhältnismäßig.

§ 22 Abs. 2 bis 4 Entwurf der Verordnung zur Umsetzung des Hessischen Lehrerbildungsgesetzes

(2) Die Prüfungskandidatin oder der Prüfungskandidat kann innerhalb eines Jahres nach Abschluss des Prüfungsverfahrens auf Antrag Einsicht in ihre oder seine Prüfungsakte nehmen. Die aktenführende Behörde bestimmt Zeit und Ort der Einsichtnahme.

(3) Die Akteneinsicht wird nur einmal gewährt und erfolgt in Gegenwart einer oder eines Bediensteten der aktenführenden Behörde. Sie soll fünf Zeitstunden nicht überschreiten und ist aktenkundig zu machen.

(4) Erhebt die Bewerberin oder der Bewerber Widerspruch gegen das Zeugnis oder den Bescheid nach § 32 Abs. 2 des Hessischen Lehrerbildungsgesetzes, werden ihr oder ihm auf Verlangen gegen Erstattung der Kosten Kopien der Prüfungsakte angefertigt.

Die Verordnung ist am 1. November 2011 in Kraft getreten. Die in Rede stehende Passage lautet jetzt:

> *§ 22 Abs. 2 Verordnung zur Umsetzung des Hessischen Lehrerbildungsgesetz*
> *(2) Für die Einsichtnahme in die Prüfungsakten gelten die allgemeinen Bestimmungen.*
> *(Die Absätze 3 und 4 sind entfallen.)*

Damit sind die kritisierten Einschränkungen des Akteneinsichtsrechts entfallen.

3.6.1.3
Weiterbildungsgesetz

Das Gesetz enthält – wie die Vorgängerfassung – keine bereichsspezifischen Regelungen zum Datenschutz. Es gilt daher, soweit im Zuge der Ausführung des Gesetzes personenbezogene Daten verarbeitet werden, das Hessische Datenschutzgesetz in der jeweils gültigen Fassung. Seit dem Inkrafttreten des Gesetzes im Jahr 2001 sind keine datenschutzrechtlichen Konflikte zutage getreten. Rein vorsorglich habe ich darauf aufmerksam gemacht, dass die in mehreren Passagen im Gesetzentwurf erwähnten Koordinierungs- und Zusammenarbeitsgebote keine hinreichende Rechtsgrundlage für ein Führen behördenübergreifender Datenbestände bieten. Doch dies lässt sich mit den Regelungen im Hessischen Datenschutzgesetz lösen, sodass sich Spezialregelungen erübrigen. Es bleibt bei der Anwendung des allgemeinen Datenschutzrechts. Dagegen war nichts einzuwenden.

Im Gesetzgebungsverfahren hat mich der Kulturpolitische Ausschuss des Hessischen Landtages noch einmal schriftlich angehört. Dabei habe ich meine Stellungnahme wiederholt und noch um folgendes Anliegen ergänzt: § 8 des Gesetzentwurfes enthält eine Beschreibung, auf welchen Gebieten die Weiterbildungseinrichtungen Bildungsangebote anbieten sollen. Da Datenschutz nicht nur eine Sache von Recht und Technik, sondern auch eine Sache von Bildung und Erziehung ist (s. Ziff. 8.7), habe ich vorgeschlagen, den Begriff „Datenschutz“ in die Aufzählung der Bildungsbereiche aufzunehmen. Der Hessische Landtag ist dem nicht gefolgt. Das Gesetz wurde am 21. November 2011 verkündet (GVBl. I S. 673).

3.6.2
Offenes Archiv in einer Außenstelle des Amtes für Lehrerbildung

Nicht nur automatisiert gespeicherte Daten sind vor unbefugtem Zugriff zu schützen. Auch bei nicht automatisiert gespeicherten Daten sind Maßnahmen zu treffen, um u. a. den Zugriff Unbefugter bei ihrer Aufbewahrung zu verhindern. Archivräume müssen so abgeschottet sein, dass nur berechtigte Personen Zugang haben.

Ein Mitarbeiter einer hessischen öffentlichen Stelle machte mich auf folgenden Sachverhalt aufmerksam: Das Archiv einer Außenstelle des Amtes für Lehrerbildung sei nicht nur von den Mitarbeitern einer anderen im gleichen Gebäude untergebrachten Behörde, sondern aufgrund eines nicht verschließbaren Notausganges für „Jedermann“ zugänglich. Zwar seien die Räume abgesehen von dem Notausgang abschließbar, doch passe jeder Dienstschlüssel zu den als Archiv verwendeten Räumen. Auch stünden die Türen oft offen, weil die Mitarbeiter das Archiv als Durchgang zu einem anderen Gebäudeteil benutzen und die Türen nicht abschließen.

In dem Archiv würden sämtliche Prüfungsakten, wissenschaftliche Hausarbeiten und Zeugnisse der 1. Staatsprüfung einschließlich Blanko-Originale aufbewahrt. Quasi könne sich jeder Student, aber auch jeder Andere mit den Unterlagen versorgen, um gefälschte Zeugnisse zu erstellen, wissenschaftliche Hausarbeiten zu kopieren oder die persönlichen Daten der Autoren zur Kenntnis zu nehmen.

Ich nahm sofort Kontakt zu dem behördlichen Datenschutzbeauftragten des Amtes für Lehrerbildung auf. Ich machte auf § 10 Abs. 3 HDSG aufmerksam, bat um Prüfung des Sachverhaltes und gegebenenfalls um sofortige Abhilfe des offenkundigen Missstandes.

> *§ 10 Abs. 3 HDSG*
> *Werden personenbezogene Daten nicht automatisiert verarbeitet, dann sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.*

Noch am selben Tag erreichte mich über den behördlichen Datenschutzbeauftragten die Stellungnahme der Leitung der Außenstelle des Amtes für Lehrerbildung. Tatsächlich hatte eine von vier Zugangstüren – sie führt über eine Wendeltreppe direkt nach außen – überhaupt keinen Schließzylinder. Andere Beschäftigte am selben Standort hatten Zugang zu den Archivräumen, weil sie über den entsprechenden Schlüssel verfügten. Dies sei bei der Zuteilung der Räume des Untergeschosses des Objektes an die Außenstelle des Amtes für Lehrerbildung übersehen worden.

Alle vier Zugangstüren zu dem Kellerabschnitt, in dem sich die Archivräume befinden, sollten nun mit separaten Zylinderschlössern ausgestattet werden. Schlüssel sollen nur diejenigen Bediensteten erhalten, zu deren Aufgaben es gehört, das Archiv zu benutzen. Die zuständige Objektleiterin des Hessischen Immobilienmanagements habe bereits den Auftrag erhalten, unverzüglich die neuen Schließzylinder einbauen zu lassen. Von der Realisierung der veranlassten Maßnahmen habe ich mich überzeugt. Der Missstand war damit umgehend abgestellt.

Von einer Beanstandung nach § 27 HDSG habe ich abgesehen.

3.6.3
Akquise einer Sparkasse an einer Schule

Jahrelang übermittelte eine Schule die Adressen der jeweils neu eingeschulten Kinder an eine Sparkasse, die diese Daten zu Werbezwecken verwendete. Die Datenübermittlung war unzulässig und wurde abgestellt.

Die Mutter eines im August eingeschulten Kindes aus dem Main-Kinzig-Kreis wunderte sich über Post der Sparkasse. Die Post war direkt an das Kind adressiert. In dem Brief bezog sich die Sparkasse auf die gerade erfolgte Einschulung und stellte die Vorzüge eines Sparkontos dar. Die Mutter informierte mich über diesen Sachverhalt und fragte, ob es in Ordnung sei, dass die Sparkasse über die Adresse ihres Kindes und die Information verfügt, dass ihr Kind gerade eingeschult worden war. Sie vermutete, die Schule habe die Information übermittelt.

Meine Feststellungen bestätigten diese Vermutung. Die Sparkasse räumte unumwunden ein, es handele sich um Datenmaterial, das die Schule eigenständig bereitgestellt habe. Die Schule habe eine Übersicht der aufgenommenen Schüler inklusive der Einteilung in die Klassenverbände mit den Anschriften übergeben. Die Aushändigung sei in Form einer Liste im Rahmen eines Besuches einer Kundenberaterin erfolgt, die zur Kundenpflege Lehrerkalender an das Kollegium überbracht habe.

Rechtsgrundlage der Datenverarbeitung in Schulen ist § 83 Abs. 1 Schulgesetz. Danach dürfen u. a. Schulen personenbezogene Daten der Schülerinnen und Schüler verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und für einen jeweils damit verbundenen Zweck erforderlich ist.

§ 83 Abs. 1 HSchG

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, soweit die Kenntnis der Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist.

In der von mir erbetenen Stellungnahme antwortete mir die Schulleiterin sehr betroffen. Sie habe erst im Laufe des Jahres die Leitung der Schule übernommen und nun entsetzt festgestellt, dass die beschriebene Praktik dort tatsächlich seit Jahren so geübt wurde. Sie habe diese Praktik sofort untersagt. Sie versicherte mir, auf dem in Kürze stattfindenden Elternabend die Eltern aller betroffenen Schüler über die Fehlleistung zu informieren und sich zu entschuldigen. Die Mutter informierte ich entsprechend. Sie bedankte sich kurz darauf und bestätigte die ausführliche Information durch die Schule und die Entschuldigung.

Die Sparkasse habe ich aufgefordert, die Daten der Schülerinnen und Schüler unverzüglich zu löschen, die Löschung schriftlich zu bestätigen und ihre Geschäftspraktiken hinsichtlich der Datenerhebung an Schulen zu korrigieren.

Die Sparkasse kam meinen Verlangen nach. Sie bestätigte die Löschung der Daten und erklärte, Datenerhebungen künftig nur mit dem Einverständnis der Erziehungsberechtigten vorzunehmen. Am Markt gewonnene Daten werden nur noch verarbeitet, wenn die Datenerhebung zweifelsfrei im Auftrag des Kunden bzw. der gesetzlichen Vertreter erfolgt ist.

Ich habe der Sache damit sein Bewenden gelassen.

3.6.4
Akquise einer Krankenkasse an einer Schule

Die Erklärung eines Schülers bzw. einer Schülerin mit der Verarbeitung personenbezogener Daten einverstanden zu sein, bedarf der hinreichenden Einsichtsfähigkeit in die Tragweite dieser Entscheidung. Ist diese nicht vorhanden, sind darauf basierende Datenerhebungen und Datenübermittlungen unzulässig.

Der Vater eines Schülers einer südhessischen Schule machte mich darauf aufmerksam, dass an einer Schule im Odenwald ein Sehtest durch eine Ersatzkrankenkasse durchgeführt wurde. Im Zusammenhang mit dem Test

waren die Schülerinnen und Schüler der 5. bis 12. Klasse gehalten, freiwillig Angaben zu ihrem Namen, Anschrift, E-Mail-Adresse, Telefonnummer, Krankenkasse und zum Berufswunsch zu machen. Der Betreffende wunderte sich, dass er nicht vorab über die Befragung seines minderjährigen Kindes informiert worden ist und seine Einwilligung dazu eingeholt wurde.

In der von mir erbetenen Stellungnahme des Schulleiters zu dem vorgebrachten Sachverhalt führte dieser aus, im Rahmen der Gesundheitsvorsorge würden seit mehr als zehn Jahren Sehtests für alle Schülerinnen und Schüler an der von ihm geleiteten Schule stattfinden. Sachkundiger externer Kooperationspartner sei jeweils die Ersatzkrankenkasse, welche die Sehtests immer zur vollen Zufriedenheit und ohne Beanstandungen durchführte. Auch in diesem Jahr waren Sehtests für alle Schülerinnen und Schüler der Jahrgangsstufen 5 bis 12 vereinbart. Weil der Ablauf bisher immer völlig unproblematisch war, wurde wohl im Vorfeld versäumt, das Verfahren genauer zu kontrollieren und zu kommunizieren.

Grundsätzlich können zwar auch minderjährige Schülerinnen und Schüler in die Verarbeitung ihrer Daten einwilligen. Es kommt aber immer darauf an, ob sie psychisch und intellektuell in der Lage sind, die Tragweite einer solchen Entscheidung einzuschätzen. Fehlt die Einsichtsfähigkeit, bedarf es der Einwilligung des Erziehungsberechtigten. Eine feste Altersgrenze, ab der Jugendliche als hinreichend einsichtsfähig gelten, gibt es nicht. Ab einem Alter von 14 bis 15 Jahren kann in der Regel vermutet werden, dass die Einsichtsfähigkeit gegeben ist. Bei jüngeren Schülerinnen und Schülern gilt die gegenteilige Regelvermutung. Im vorliegenden Falle wurden die Einverständniserklärungen bei den Schülerinnen und Schülern ab der 5. Jahrgangsstufe eingeholt. Diese waren also über mehrere Jahrgänge hinweg ungültig, da die Einwilligenden erst 13 Jahre alt und jünger waren.

Zum Zeitpunkt meiner Ansprache hatte der Schulleiter aufgrund von Beschwerden Betroffener bereits selbst festgestellt, dass die Datenerhebung bei den unteren Jahrgangsstufen unzulässig war. Doch auch bei den nachfolgenden Jahrgängen wäre es wünschenswert gewesen, die Erziehungsberechtigten über den Sehtest und die Datenerhebung zu informieren.

Im Übrigen muss bei der Einwilligung gemäß § 7 Abs. 2 HDSG auf den Verwendungszweck der Daten hingewiesen werden. Die Betroffenen sind unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und jederzeit mit Wirkung für die Zukunft widerrufen können.

§ 7 Abs. 2 HDSG

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

Im vorliegenden Falle war zwar auf die Freiwilligkeit hingewiesen worden, ebenso, dass mit den Daten Aufklärungs- und Beratungsangebote verbunden sein sollen, der Hinweis auf die Widerrufsmöglichkeit fehlte jedoch. Insoweit waren also auch die Einwilligungserklärungen der hinreichend einsichtsfähigen Schülerinnen und Schüler fehlerhaft.

Der Schulleiter hatte deshalb die Datenerhebungsbögen bereits eingezogen und in seinem Dienstzimmer verwahrt, um sie der Vernichtung zuzuführen. Zudem hatte er von der Ersatzkrankenkasse die schriftliche Erklärung eingeholt, dass die Schülerdaten weder gespeichert oder weitergegeben noch irgendwie sonst verwendet werden.

Abgesehen von der unzulässigen Datenerhebung konnte also im konkreten Fall festgestellt werden: „Gerade noch mal gut gegangen“. Es war konsequent, die unzulässig erhobenen Daten zu vernichten. Zu unzulässigen Datenweitergaben oder Datenspeicherungen kam es nicht mehr. Auch hier habe ich von einer Beanstandung nach § 27 HDSG abgesehen.

3.6.5
Veröffentlichung von allen Absolventen einer Fakultät einer hessischen Universität

Eine hessische Universität veröffentlichte personenbezogene Daten aller Absolventen einer bestimmten Fakultät. Für diese Veröffentlichung gibt es keine Rechtsgrundlage; sie war daher unzulässig.

Eine betroffene Person informierte mich darüber, dass eine hessische Universität zur Feier des 150-jährigen Bestehens einer Fakultät einen Festakt veranstaltet hat. Zu dem Festakt wurde eine Festschrift herausgegeben. In der Festschrift wurden personenbezogene Daten der Studierenden der entsprechenden Fachrichtung der letzten ca. 50 Jahre aufgeführt. Genannt sind: Name, Vorname, Geburtsdatum, Geburtsort, Datum des Vordiploms

und Datum des Diploms. Insgesamt wurden die Daten von 718 Personen veröffentlicht. Auf diese Weise waren nicht nur die Namen und Geburtsdaten offenbart, sondern auch, wie lange die Absolventen zwischen Vordiplom und Diplom studierten bzw. ob sie überhaupt Vordiplom und Diplom an dieser Universität erreicht hatten. Die Festschrift wurde während der Festveranstaltung an Interessierte verkauft. Auf der Webseite, auf der über den Festakt berichtet wurde, befand sich die Anschrift des Institutes, bei dem die Festschrift nachträglich erworben werden konnte. Das Einverständnis der Betroffenen – so die Person, die sich an mich wandte – war nicht eingeholt worden.

Hochschulen dürfen gem. § 55 Abs. 4 Hochschulgesetz zur Erfüllung ihrer Aufgaben und den jeweils damit verbundenen Zweck die erforderlichen personenbezogenen Daten u. a. der Studierenden verarbeiten. Umfang und Einzelheiten regelt eine Verordnung.

§ 55 Abs. 4 Hochschulgesetz

Die Hochschule verarbeitet zur Erfüllung ihrer Aufgabe und der damit jeweils verbundenen Zwecke die erforderlichen personenbezogenen Daten der Bewerberinnen und Bewerber, Studierenden, Gasthörerinnen und -hörer und Prüfungskandidatinnen und -kandidaten. Diese sind verpflichtet, die erforderlichen Angaben zu machen und Unterlagen vorzulegen. Die Ministerin oder der Minister für Wissenschaft und Kunst wird ermächtigt, durch Rechtsverordnung Umfang und Einzelheiten der personenbezogenen Datenverarbeitung einschließlich der Übermittlung an Dritte zu regeln.

Die Veröffentlichung personenbezogener Daten aller Absolventen einer Fakultät ist zur Aufgabenerfüllung einer Hochschule nicht erforderlich. Auch die in § 55 Abs. 4 Hochschulgesetz genannte Verordnung (Verordnung über das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation, das Studium als Gasthörerin oder Gasthörer, das Teilzeitstudium und die Verarbeitung personenbezogener Daten der Studierenden an den Hochschulen des Landes Hessen – Hessische Immatrikulationsverordnung, HImVO) enthält dazu keine Rechtsgrundlage. In Ermangelung einer Rechtsgrundlage wäre daher die Veröffentlichung der personenbezogenen Daten nur zulässig gewesen, wenn die Betroffenen gem. § 7 Abs. 1 Nr. 3 HDSG eingewilligt hätten.

Ich bat die Universität um eine Stellungnahme zu dem Sachvortrag. Leider ist der geschilderte Sachverhalt zutreffend – so der Präsident der Universität – in seiner Stellungnahme. Mit Bedauern räumte er ein, es im Rahmen der Vorbereitungen des Jubiläums versäumt zu haben, die Zustimmung der Betroffenen einzuholen. Die Verbreitung der Festschrift sei umgehend eingestellt worden. Bereits in Umlauf gebrachte Exemplare wurden zurückerbeten und zusammen mit der vorhandenen Restauflage vernichtet. Dies gelang bei ca. 120 von insgesamt 200 Exemplaren der Festschrift. Der Rest, ca. 80 Exemplare, geriet in Umlauf und konnte nicht zurückgeholt werden. Der Präsident der Universität versicherte, im Zusammenhang mit künftigen Jubiläen im Vorfeld aktiv auf datenschutzrechtliche Rahmenbedingungen hinzuweisen.

Die Person, die mich auf den Sachverhalt aufmerksam gemacht hat, habe ich entsprechend informiert und ihr bestätigt, dass sie in ihren datenschutzrechtlichen Belangen verletzt wurde. Die Universität hat den Fehler eingeräumt, ihr Bedauern ausgedrückt und weitgehend Vorkehrungen getroffen, Wiederholungsfälle zu vermeiden. Ich habe deshalb von einer Beanstandung gemäß § 27 HDSG abgesehen.

3.7 Forschung und Statistik

3.7.1
Datenschutzrechtliche Vorgaben für die Lärmwirkungsstudie im Umfeld des Frankfurter Flughafens

Ein Konsortium von Lärmwirkungsforschern wurde mit einer Lärmwirkungsstudie beauftragt. Für die Studie wurden zunächst die Meldedaten der Einwohnerinnen und Einwohner der betroffenen Region benötigt, damit diese um ihre Teilnahme an der Studie gebeten werden können. Meine Dienststelle hat den Auftraggeber und das Konsortium hinsichtlich des Datenschutzkonzepts für die Studie beraten und die Meldebehörden wie auch später anfragende Bürgerinnen und Bürger über das Ergebnis informiert.

3.7.1.1
Inhalt der Studie und beteiligte Institutionen

Die vom Land Hessen gegründete Gemeinnützige Umwelthaus GmbH (UNH, www.forum-flughafen-region.de/forum/umwelthaus) hat ein Konsortium von Lärmwirkungsforschern beauftragt, eine Lärmwirkungsstudie (NORAH – Noise Related Annoyance, Cognition, and Health) zu den gesundheitlichen Auswirkungen des Flug- sowie Schienen- und Straßenlärms im Umfeld des Frankfurter Flughafens in den Jahren 2011 bis 2014 durchzuführen. Ziel der Studie ist es, eine möglichst repräsentative und wissenschaftlich abgesicherte Beschreibung der Auswirkungen des Lärms von Flug-, Schienen- und Straßenverkehr im Rhein-Main-Gebiet auf die Gesundheit und Lebensqualität der betroffenen Wohnbevölkerung zu erhalten. Mehrere Forschungs- und Fachinstitutionen der Medizin, Psychologie,

Sozialwissenschaft, Akustik und Physik haben sich zu einem Forschungskonsortium zusammengeschlossen, um der gesamtheitlichen Erforschung der Wirkung von Verkehrslärm nachzugehen.

Das mir im Frühjahr vorgelegte Konzept sah Folgendes vor:

In einem ersten Schritt soll die UNH ca. 2,7 Millionen Datensätze von den Meldeämtern des Rhein-Main-Gebiets erhalten. Die von den Meldeämtern benötigten Datensätze enthalten jeweils

- Name und Adresse
- Geburtsjahr
- Jahr des Zuzugs
- Geschlecht

der Einwohnerinnen und Einwohner. Die UNH führt die Meldedaten mit Geodaten und Fluglärm-Pegeln zusammen und übermittelt diese 2,7 Millionen Datensätze an das Sozialwissenschaftliche Umfragezentrum GmbH (SUZ, www.suz-umfragen.de/) in Duisburg, ferner übermittelt sie auszugsweise aus Teilgebieten der ausgewählten Region die Datensätze an das Deutsche Zentrum für Luft- und Raumfahrt e. V. in Köln (http://www.dlr.de/dlr/desktopdefault.aspx/tabid-10002).

Das SUZ schickt unter einer ID-Nummer, ohne Namen oder Adresse, den Fluglärmpegel und den Gemeindenamen an das Zentrum für angewandte Psychologie, Umwelt- und Sozialforschung in Hagen (ZEUS GmbH). Ein weiterer Konsortialpartner, Möhler & Partner Ingenieure AG in München (MOPA), erhält vom SUZ die ID-Nummer und die Geodaten. Anhand von Daten zum Straßen- und Schienenverkehr berechnet MOPA den Lärmpegel für Schienen- und Straßenverkehr zu den Geodaten. Die ID-Nummer und den Schienen- und Straßenverkehrspegel, nicht die Geodaten, sendet MOPA an ZEUS. Dort werden Lärmklassen nur an Hand der Lärmpegel gebildet; es sind zu einer ID-Nummer keine Namen, Adressen oder Geodaten bekannt, nur die Gemeinde. Anschließend werden aus verschiedenen Lärmklassen die ID-Nummern potenzieller Studienteilnehmer unter Berücksichtigung der Gemeinde mit Zufallsziehung ausgewählt. An das SUZ gehen dann die ausgewählten ID-Nummern je Studie. Das SUZ schreibt nun die ausgewählten Personen an, ob sie bereit sind, an der Studie teilzunehmen.

An der Durchführung der Studie sind zusätzlich zu dem SUZ und der DLR verschiedene weitere Institutionen in verschiedenen Bundesländern mit je speziellen Aufgabenstellungen beteiligt. Die Studie beinhaltet insgesamt auf der Grundlage einer Einwilligung der Betroffenen

- telefonische Basisbefragungen von Einwohnern bis 2014 zweimal jährlich und
- (auf der Grundlage einer gesonderten Einwilligungserklärung) von einem Teil der Einwohner medizinische Untersuchungen, d. h. eine Analyse der durch Verkehrslärm beeinflussten Schlafqualität und des Blutdrucks, sowie
- zu einem späteren Zeitpunkt auch kinderpsychologische Untersuchungen und eine Auswertung von Krankenkassendaten.

Alle an der Durchführung der Studie beteiligten Institutionen haben einen Kooperationsvertrag geschlossen.

3.7.1.2 Datenschutzrechtliche Vorgaben für die Übermittlung der Meldedaten

Im Frühjahr 2011 habe ich zahlreiche Anfragen von Meldebehörden erhalten bezüglich der Zulässigkeit der Übermittlung der Meldaten an die UNH. Das Hessische Meldegesetz (HMG) erlaubt unter bestimmten Voraussetzungen eine Übermittlung von Meldedaten für ein bestimmtes Forschungsvorhaben ohne Einwilligung der Betroffenen. Im konkreten Fall kommt die Regelung in § 35 Abs. 7 Satz 2 HMG in Betracht. Nach dieser Bestimmung ist eine Übermittlung zulässig, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Forschungszweck auf andere Weise nicht erreicht werden kann.

§ 35 Abs. 7 HMG

Zum Zwecke unabhängiger wissenschaftlicher Forschung dürfen die Meldebehörden personenbezogene Daten ohne Einwilligung der Betroffenen nur für bestimmte Forschungsvorhaben übermitteln, soweit die schutzwürdigen Belange der Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung der Betroffenen bedarf es nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Forschungszweck auf andere Weise nicht erreicht werden kann. Sobald der Forschungszweck dies erlaubt, sind die Daten und Hinweise, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern und nach Erreichen des Forschungszwecks zu löschen.

Damit die Forscher die Studie durchführen können, müssen sie die Einwohnerdaten aller erwachsenen Personen der betroffenen Region haben, um daraus eine repräsentative Stichprobe ziehen und die dadurch ausgewählten Einwohner dann um Teilnahme bitten zu können. Eine andere Verfahrensweise ist nicht realisierbar. Ein erhebliches überwiegendes öffentli-

ches Interesse an der Durchführung des Forschungsvorhabens kann allerdings nur dann bejaht werden, wenn ein Datenschutzkonzept für das Forschungsvorhaben vorliegt, das sicherstellt, dass

- die beteiligten Forschungsinstitutionen personenbezogene Daten jeweils nur in dem Umfang und für den Zeitraum verarbeiten, für den sie sie tatsächlich benötigen und
- von allen beteiligten Forschungsinstitutionen angemessene Datensicherheitsmaßnahmen gegen den Zugriff Unbefugter getroffen werden.

3.7.1.3
Beratungen meiner Dienststelle

Zum Zeitpunkt der Anschreiben des Konsortiums an die Meldebehörden bzw. der an meine Dienststelle gerichteten Anfragen waren zwar einige Entscheidungen über geplante Datensicherheitsmaßnahmen bereits getroffen worden, es lag jedoch noch kein detailliertes Datenschutzkonzept vor. Insbesondere war auch nicht hinreichend verbindlich schriftlich festgelegt, welche an dem Konsortium beteiligte Institution für welchen Zweck welche Daten wie lange erhält und welche der Institutionen für welche Datenschutzmaßnahmen verantwortlich ist. Meine Dienststelle hat daraufhin zunächst mit dem Auftraggeber der Studie (UNH) und Vertretern des Konsortiums ein eingehendes Gespräch geführt, in dem die für das Forschungsvorhaben erforderlichen Datenflüsse gemeinsam analysiert und zusammengestellt wurden; ferner, welche Institution in welchem Umfang welche Daten für ihre Aufgaben benötigt (z. B. personenbezogene Daten oder nur ID-Nummern, Datensätze mit Adressen, mit Geodaten, mit Lärmdaten etc.) und wer welche Datenschutzmaßnahmen zu treffen hat. Es folgten weitere mündliche und schriftliche Beratungen meiner Dienststelle. Im Ergebnis lag Anfang Mai ein mit mir abgestimmtes und von dem Auftraggeber der Studie und von allen am Konsortium beteiligten Auftragnehmern unterschriebenes detailliertes Datenschutzkonzept vor.

Das detaillierte Datenschutzkonzept sieht insbesondere vor, dass

- die 2,7 Millionen Datensätze in der UNH nach Eingangsbestätigung vom SUZ und von der DLR gelöscht werden,
- die nicht gezogenen ca. 2,2 Millionen Datensätze nach Abschluss der Stichprobenziehung Anfang 2012 in keiner der am Konsortium beteiligten Institutionen mehr vorhanden sind,
- die UNH und alle am Konsortium beteiligten Institutionen die ihnen jeweils vorliegenden Daten ausschließlich strikt zweckgebunden für die Studie verwenden und alle Verarbeitungsschritte nachvollziehbar und revisionsfähig machen sowie
- die UNH und alle am Konsortium beteiligten Institutionen sich verpflichten, in ihrem Verantwortungsbereich zum Schutz der Personendaten angemessene Sicherungsmaßnahmen zu treffen.

Nach Unterzeichnung des Datenschutzkonzepts durch die UNH sowie aller am Konsortium beteiligten Institutionen habe ich der UNH, dem Konsortium sowie den Meldebehörden mitgeteilt, dass die Voraussetzungen des § 35 Abs. 7 HMG für eine Übermittlung der Meldedaten für die Lärmstudie jetzt vorliegen und die Daten übermittelt werden können. Entsprechend habe ich Bürgerinnen und Bürger informiert, die sich nach Erhalt eines Anschreibens des Konsortiums bei mir darüber informieren wollten, ob ihre Meldedaten rechtmäßig an das Konsortium weitergegeben wurden.

Für die konkrete Umsetzung der im Datenschutzkonzept festgelegten Datenschutzmaßnahmen bundesweit in den einzelnen am Konsortium beteiligten Stellen sind die jeweils für diese Stellen zuständigen Datenschutzbeauftragten bzw. Datenschutzaufsichtsbehörden zuständig.

3.7.1.4
Teilprojekt „Sekundäranalyse von Krankenkassenversicherten-Daten mit darauf aufbauender Fall-Kontroll-Studie“

Im Sommer 2011 habe ich mit der Bitte um Beratung zusätzliche Unterlagen von der Technischen Universität Dresden (Medizinische Fakultät, Institut und Poliklinik für Arbeits- und Sozialmedizin) erhalten zur Durchführung des Teilprojekts „Sekundäranalyse von Krankenkassenversichertendaten mit darauf aufbauender Fall-Kontroll-Studie“ im Rahmen von NORAH.

Geplant ist eine umfangreiche Sekundäranalyse durch die Universität Dresden von bereits bei den Krankenkassen verschiedener Kostenträger vorhandenen Versichertendaten, die den Zusammenhang zwischen der wohnortbezogenen Belastung gegenüber Fluglärm, Straßenlärm und Schienenlärm und dem Auftreten von Herz-Kreislauferkrankungen (Herzinfarkt, Herzschwäche, Schlaganfall), Krebserkrankungen (insbesondere Brustkrebs) und Depression aufzeigen soll. Berechnet werden sollen die Fluglärm-, Straßenlärm- und Schienenlärm-bezogenen Erkrankungsrisiken an Herzinfarkten, Schlaganfällen, Brustkrebs und Depressionen im Vergleich mit nicht oder gering lärmexponierten Personen. Für alle einbezogenen Versicherten (angestrebt: ca. 2 Millionen Datensätze) soll eine adressgenaue Zuordnung der Exposition gegenüber den genannten Lärmquellen erfolgen. Dabei sol-

len die Krankenkassen für die ausgewählten Versicherten eine nicht sprechende ID vergeben und an eine Vertrauensstelle die ID mit den jeweiligen Wohnadressen übermitteln. In dieser Vertrauensstelle werden die Lärmdaten auf die Wohnadressen bezogen und die IDs mit den adressbezogenen Lärmdaten an eine Auswertungsstelle (Universität Dresden) weitergeleitet, die von den Krankenkassen zu den jeweiligen ID-Nummern auch Daten über die Erkrankungsrisiken erhält.

Eine vertiefende Ermittlung der Krankheitsrisiken unter Berücksichtigung möglicher „konkurrierender" Einflussfaktoren wie z. B. Rauchverhalten, Nachtschichtarbeit etc. soll mit einer auf der Sekundäranalyse aufbauenden Fall-Kontroll-Studie durch die Universität Gießen (Institut für Hygiene und Umweltmedizin) erreicht werden: Bei alleiniger Berücksichtigung der Routinedaten der Krankenkassen sind Ergebnisverzerrungen nicht auszuschließen. Ziel der Studie ist daher eine genauere Ermittlung der lärmbezogenen Erkrankungsrisiken unter Berücksichtigung individueller Befragungsdaten z. B. zum Rauchverhalten, zur Berufstätigkeit einschließlich Nachtschichtarbeit etc. Dazu sollen aus den o. a. Versichertendatensätzen jeweils 6.000 Personen mit Neuerkrankungen an Herzinfarkt, Herzschwäche und Schlaganfall („Fälle") sowie 6.000 nicht an diesen Erkrankungen leidende Versicherte („Kontrollpersonen") gezogen werden. Insgesamt sollen also 24.000 Personen um ihre Mitwirkung an der Studie (detaillierte Befragung) gebeten und nach expliziter Einwilligungserklärung in die Fall-Kontroll-Studie einbezogen werden.

In einem ersten Schritt wurden zwischen meiner Dienststelle, dem von mir einbezogenen Hessischen Sozialministerium und der Universität Dresden datenschutzrechtlich mögliche Vorgehensweisen bei der Verwendung von Daten hessischer Krankenkassen besprochen. Es bedarf für die Datenübermittlung der Versichertendaten von den Krankenkassen einer Rechtsgrundlage. Zwar werden zu keinem Zeitpunkt die Namen der Versicherten weitergegeben, aber durch die im Rahmen der Studie verarbeiteten Adressdaten und Geodaten sowie durch den in der Auswertungsstelle verarbeiteten umfangreichen Datensatz zu den Erkrankungsrisiken etc. kann insgesamt nicht von einer vollständig anonymisierten bzw. pseudonymisierten Datenverarbeitung ausgegangen werden.

Bei Redaktionsschluss stand noch nicht fest, ob und ggf. unter welchen Voraussetzungen sich Krankenkassen und/oder private Krankenversicherungen an dem Forschungsvorhaben beteiligen, sodass eine abschließende Diskussion des Datenschutzkonzepts noch nicht möglich war.

Ich werde auch weiterhin für Besprechungen des Datenschutzkonzepts zur Verfügung stehen. Für die konkrete Umsetzung des Datenschutzkonzepts

an der Universität Dresden ist der Datenschutzbeauftragte des Landes Sachsen zuständig.

3.7.2
Volkszählung (Zensus) 2011

Die Durchführung der Volkszählung in Hessen haben meine Mitarbeiter intensiv und mit hohem Aufwand begleitet. Dabei konnte festgestellt werden, dass es im Rahmen der Verfahrensabläufe in den 33 Erhebungsstellen des Landes sowie im Zusammenhang mit der Einschaltung privater Unternehmen für den Versand der Erhebungsunterlagen und deren Aufbereitung zu keinen Unregelmäßigkeiten gekommen ist, welche das Projekt hätten in Frage stellen können. Die angetroffenen kleineren Mängel wurden umgehend abgestellt.

Ein Schwerpunkt meiner Prüftätigkeit im Berichtsjahr hatte die datenschutzrechtliche Begleitung des Zensus 2011 zum Inhalt. Bereits im Jahr 2010 hatten meine Mitarbeiterinnen und Mitarbeiter an vorbereitenden Sitzungen der Statistischen Ämter der Länder Hessen, Thüringen, Sachsen und Sachsen-Anhalt teilgenommen, um die Frage zu klären, ob eine Auftragsdatenverarbeitung der Dienstleistungen Postversand und Aufbereitung der Erhebungsbögen, statistikrechtlich möglich ist. Meine Bewertung hierzu habe ich im 39. Tätigkeitsbericht (Ziff. 3.3.4) dokumentiert und die geplante Verfahrensweise für zulässig erachtet.

Um eine Vorstellung über den Prüfumfang und den damit verbunden Aufwand zu erhalten, ist die Darstellung einiger Zahlenwerte hilfreich: So waren 21 Arbeitstage erforderlich, um die 33 hessischen Erhebungsstellen zu überprüfen. Hinzu kamen neun Prüfungstermine bei externen Dienstleistern mit Standorten in Niedersachsen, Bayern und Sachsen. In diesem Zusammenhang haben meine Mitarbeiter mehr als 6.000 Kilometer zurückgelegt und eine Vielzahl Prüfprotokolle geschrieben, Gesprächsvermerke gefertigt sowie schriftliche Korrespondenz mit den geprüften Einrichtungen abgewickelt. Schließlich galt es, mit dem Hessischen Statistischen Landesamt (HSL) einen regelmäßigen Erfahrungsaustausch zu praktizieren, um sich gegenseitig über neue Entwicklungen und Erkenntnisse zu informieren. Vier Termine fanden hierzu im Jahr 2011 statt.

3.7.2.1
Erhebungsstellen

In den 21 hessischen Landkreisen, den Großstädten sowie den Städten mit Sonderstatus (z. B. Bad Homburg, Rüsselsheim) wurden bereits Ende des

Jahres 2010 Statistikstellen eingerichtet. Rechtliche Grundlage hierfür ist § 10 Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781 ff.) und das Hessische Ausführungsgesetz zum Zensus 2011 und Gesetz zur Änderung des Hessischen Landesstatistikgesetzes vom 23. Juni 2010 (GVBl. Teil I, S. 178 ff.). Für die Einrichtung und den Betrieb dieser Stellen, die für die Abwicklung der Haushaltsbefragung verantwortlich waren und welche die Zusatzerhebungen zu organisieren hatten, war vom HSL eine „Empfehlung" erarbeitet worden. Der Umsetzung dieser Vorgaben hinsichtlich der personellen, administrativen und organisatorischen Abwicklung des Zensus 2011 galt mein Prüfinteresse ebenso wie der technischen Ausgestaltung der Anbindung zum Statistikamt Nordrhein-Westfalen in Düsseldorf, welches im Rahmen der Verbundorganisation der Landesstatistikämter zentral die Programmentwicklung der Haushaltsbefragung und die Speicherung dieser Daten übernommen hatte.

3.7.2.1.1
Trennung von anderen Verwaltungsstellen

Die Trennung der Erhebungsstellen von den anderen Bereichen der Verwaltung war eine der wesentlichen Vorgaben des Gesetzgebers im Zusammenhang mit der Durchführung des Zensus. Nach § 6 Abs. 1 des Ausführungsgesetzes waren die Erhebungsstellen für die Dauer der Bearbeitung und Aufbewahrung von Einzelangaben räumlich und organisatorisch von anderen Verwaltungsstellen zu trennen, mit eigenem Personal auszustatten und gegen den Zutritt unbefugter Personen hinreichend zu schützen.

Die Prüfung durch meine Mitarbeiter hat ergeben, dass diesem Anspruch grundsätzlich Genüge getan war. Allerdings gab es Lösungen, die sehr anspruchsvoll und kreativ waren, in anderen wenigen Fällen erreichte man die Abschottung unter Bedingungen, die datenschutzrechtlich noch akzeptabel erschienen.

3.7.2.1.2
Räumliche Situation

Die von den verantwortlichen Stellen in Städten und Landkreisen entwickelten Lösungen waren – wie nicht anders zu erwarten – sehr unterschiedlich. So gab es in wenigen Fällen Räume im Überfluss – der Landkreis Gießen nutzte eine alte Schule als Erhebungsstelle, die Stadt Rüsselsheim hatte ein ganzes Stockwerk eines älteren Gebäudes eingerichtet – in anderen Fällen war der Mangel unübersehbar (so der Landkreis Darmstadt-Dieburg, der als eine der Stellen mit den zahlenmäßig umfangreichs-

ten Haushaltsbefragungen über nur einen einzigen Raum verfügte, in dem die Bearbeitung der Bögen ebenso stattfinden musste wie die Abwicklung von Publikumsverkehr oder die Kommunikation mit den Erhebungsbeauftragten). Durchweg wurden jedoch die Vorgaben hinsichtlich der Ausgestaltung der Räume unter statistik- und datenschutzrechtlichen Belangen im Wesentlichen eingehalten.

3.7.2.1.3
Organisation

Das HSL hatte für die Erhebungsstellen eine Musterdienstanweisung entwickelt und mit meiner Dienststelle inhaltlich abgestimmt. Fast ausnahmslos alle Organisationseinheiten haben dieses Papier zur Grundlage der Tätigkeit der Erhebungsstelle gemacht. Neben Hinweisen zu personellen Erfordernissen hinsichtlich des Erhebungsstellenpersonals sowie der Erhebungsbeauftragten, der Ausgestaltung und Einrichtung der Erhebungsstellen oder der Stellung innerhalb der Verwaltung enthält das Papier auch Empfehlungen zur technischen Ausgestaltung der Erhebungsstelle (Einzelheiten s. unter Ziff. 3.7.2.1.9). Dieser empfehlende Charakter der Unterlage führte offensichtlich dazu, dass in einigen Städten und Landkreisen die Regelungen ungeachtet der eindeutigen, gesetzlichen Vorgaben als unverbindlich angesehen wurden und in Folge dessen die Umsetzung zu locker gehandhabt wurde. Deshalb muss eine der Konsequenzen für die Zukunft lauten, eine Verbindlichkeit herzustellen, um die ausführenden Stellen auf Grundlage der gesetzlichen Regelungen von vorneherein auf die für notwendig erachteten technischen, organisatorischen und personellen Erfordernisse festzulegen.

3.7.2.1.4
Der Klassiker: Offener Zugang zu ausgefüllten Bögen zum Prüfzeitpunkt

Alle datenschutzrechtlich relevanten Einzelheiten darzustellen, die in den 33 Erhebungsstellen angetroffen bzw. festgestellt wurden, würde den Rahmen der Berichterstattung bei Weitem sprengen. Dennoch gilt es, ein Ereignis besonders hervorzuheben. Nicht, um den dortigen Leiter oder das Erhebungsstellenpersonal an den Pranger der Öffentlichkeit zu stellen. Vielmehr soll der Fall auf seine klassische Weise deutlich machen, wie oft der Teufel im Detail steckt und wie schnell ein vermeintlich kleiner Organisationsfehler zu erheblichen Risiken führt.

Konkret ging es um den Zugang zur Erhebungsstelle, der ausschließlich einem berechtigten Personenkreis eingeräumt war. Entsprechend musste

die Schlüsselgewalt geregelt werden. Ein Zutritt des Reinigungsdienstes sollte ausschließlich nur in Anwesenheit des Erhebungsstellenpersonals möglich sein. Im Landkreis Offenbach war dies so aber nicht geregelt. Der Dienst verfügte über einen eigenen Schlüssel zu den Räumen der Erhebungsstelle. Zum Ende meiner Prüfung hin an einem späten Freitag Nachmittag, als sich die Kreisverwaltung bereits geleert hatte, entdeckten meine Mitarbeiter die weit offen stehende Tür zu dem Raum, in dem die bislang eingegangenen ausgefüllten Erhebungsbögen gelagert waren. Weit und breit waren weder Erhebungsstellenpersonal noch die Mitarbeiterinnen des Reinigungsdienstes zu sehen. Kein Frage, dass der Erhebungsstellenleiter über die angetroffene Situation alles andere als begeistert war. Doch wie kam es dazu? Die Mitarbeiterinnen und Mitarbeiter der Erhebungsstelle, die im Raum tätig waren, hatten Dienstschluss und sich ins Wochenende begeben. Die Reinigungskräfte schwärmten am späten Freitagnachmittag aus, schlossen die Türen auf und widmeten sich zunächst anderen Aufgaben. Von den besonderen Anforderungen hinsichtlich der Abschottung sowie des Zugangs zur Statistikstelle bzw. der einschlägig genutzten Räume hatten die Kräfte keine Kenntnis. Die Konsequenzen wurden schnell gezogen: die Erhebungsstelle bekam eine neue Schließanlage und der Putzdienst konnte ab sofort nur noch in Anwesenheit des Erhebungspersonals die Reinigung der Räume vornehmen.

3.7.2.1.5
Erhebungsstellenleitung

Nach § 4 des Ausführungsgesetzes waren für die Erhebungsstellen eine Leitung und deren Stellvertretung zu bestellen. Bis auf eine Erhebungsstelle war diesem wichtigen gesetzlichen Erfordernis durch die förmliche Zuweisung der Aufgabe und Bestellung durch den Oberbürgermeister oder den Landrat entsprochen worden. Hinsichtlich des Anforderungsprofils musste gewährleistet sein, dass die Leitungsfunktion nur von Mitarbeitern innerhalb der Verwaltung wahrgenommen wurde, die „unkritischen“ Verwaltungseinheiten angehörten. Der Gesetzgeber hatte ausdrücklich ausgeschlossen, dass aus bestimmten Bereichen wie z. B. der Vollstreckung, den Baubehörden, den Meldeämtern, den Ausländerbehörden Personal in der Erhebungsstelle eingesetzt wird. Dieser Vorgabe wurde von allen Stellen Rechnung getragen.

Kritikwürdig war anderseits jedoch der Umstand, dass die betroffenen Erhebungsstellenleiter oder deren Vertreter teilweise auch ihren eigentlichen Aufgaben in der Verwaltung nachzukommen hatten und hier eine nicht unerhebliche Doppelbelastung festzustellen war. Statistikrechtlich war eine der-

artige Verfahrensweise nicht unzulässig, in der Sache selbst jedoch deplaziert. So wunderte es nicht, dass in einigen Fällen die Betroffenen an die Grenze ihrer Belastbarkeit gelangten bzw. diese überschritten.

In einigen wenigen Fällen (z. B. Landkreis Bergstraße, Stadt Bad Homburg) rekrutierte die Verwaltungsspitze ehemalige, ausgeschiedene Mitarbeiter der Verwaltung und belastete für diese Funktion den eigenen Verwaltungskörper nicht.

3.7.2.1.6
Erhebungsstellenpersonal

Was für die Erhebungsstellenleitung galt, war auch für das dort tätige Personal umzusetzen: aus sensibel einzuschätzenden Bereichen der Verwaltung sollten keine Mitarbeiter rekrutiert werden. Erfreulich, dass es hier keinen Anlass zur Kritik gab. Auch die Verpflichtung der Mitarbeiter auf die statistische Geheimhaltung war – bis auf den Landkreis Darmstadt-Dieburg – durchweg erfolgt. In nicht wenigen Fällen wurde externes Personal auf Zeit eingestellt. Hier erfolgte die Überprüfung u. a. der Zuverlässigkeit durch die rechtlich zulässige Vorlage eines Bundeszentralregisterauszuges.

3.7.2.1.7
Erhebungsbeauftragte

In der Begründung zu § 9 des Ausführungsgesetzes (Bestellung und Beaufsichtigung der Erhebungsbeauftragten) führte der Hessische Gesetzgeber zu Recht aus, dass das Vertrauen der Bürgerinnen und Bürger in die rechtmäßige und ordnungsgemäße Durchführung der Erhebungen nicht zuletzt von dem Vertrauen abhänge, welches diese in die Person des Erhebungsbeauftragten setzten. Deshalb müssten die Erhebungsbeauftragten sorgsam ausgewählt werden. Beschwerden im Zusammenhang mit dem Einsatz der Erhebungsbeauftragten sind nur einige wenige an mich herangetragen worden. In dem Bemühen, den Erhebungsstellenleitungen möglichst viel an Hilfestellung zukommen zu lassen und praktische Handlungsanleitungen zu erstellen, schoss das HSL aber einige Male über das Ziel hinaus.

3.7.2.1.7.1
Speicherung von Ausweiskopien

So erreichte meine Mitarbeiter die Anfrage der Statistiker, ob die Fertigung von Ausweiskopien der Erhebungsbeauftragten auf Einwände stoße. Solche musste ich geltend machen, weil ich keine Rechtsgrundlage hierfür

erkennen konnte. Zwar waren die Erhebungsstellen zu einer Identitätsprüfung angehalten und es war durchaus angemessen, sich den Personalausweis vorlegen zu lassen. Gleichwohl hat die Anfertigung einer Kopie des Dokuments sowie der Ablage in den Akten der Erhebungsstelle eine zusätzliche datenschutzrechtliche Qualität, die weder durch das Hessische Sicherheitsüberprüfungsgesetz (HSÜG) noch das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) abgedeckt ist. Leider waren zum Zeitpunkt der Anfrage anders lautende Hinweise des HSL an die Erhebungsstellen ergangen, so dass man in einer großen Zahl von Stellen die Kopien anfertigte. Nach meiner Intervention wies das HSL zwar die Erhebungsstellen an, die Kopien zu vernichten. Gleichwohl musste ich im Rahmen meiner Prüfungen feststellen, dass einige Stellen die Kopien von Ausweispapieren in den Akten abgelegt hatten und diese erst nach Aufforderung durch meine Mitarbeiter vernichteten.

3.7.2.1.7.2
Überprüfung durch das Landeskriminalamt

Nur durch einen Zufall bin ich im Verlauf meiner Prüfungen darauf aufmerksam geworden, dass die amtliche Statistik auch in einem anderen Zusammenhang massiv in die Rechte der Betroffenen Eingriff nahm. Das Motiv war offensichtlich eine bundesweit beachtete Kampagne rechtsradikaler Gruppen. Diese hatten angekündigt, die Gruppe der Erhebungsbeauftragten mit eigenen Mitgliedern unterwandern und den Zensus sabotieren zu wollen. Um eine derartige Konstellation von Anfang an auszuschließen, bot das HSL den Erhebungsstellen eine Sicherheitsüberprüfung der Erhebungsbeauftragten durch das Hessische Landeskriminalamt (HLKA) an. Von den 33 Erhebungsstellen war es nur die des Lahn-Dill-Kreises, welche die Namen und Anschriften von mehr als 40 Personen an das HSL übermittelte. Von dort wurden die Angaben an das HLKA weitergeleitet und von den Polizeicomputern gerastert. In zwei Fällen wurde man fündig: zum einen ging es um einen möglichen Internetbetrug, zum anderen um einen umgestoßenen Blumenkübel. Ich habe das Verfahren gegenüber dem HSL sofort kritisiert, von einer Beanstandung jedoch abgesehen. Gleichzeitig habe ich die Löschung der Daten verlangt. Dem ist das HSL unmittelbar nachgekommen. Eine Weiterleitung der Erkenntnisse an den Lahn-Dill-Kreis erfolgte nicht. Auch wenn an die Seriosität und Zuverlässigkeit der Erhebungsbeauftragten ein hoher Maßstab anzulegen ist, war die Maßnahme des HSL unverhältnismäßig und durch keine Rechtsgrundlage gedeckt.

3.7.2.1.8
Besucher

Gesetzlich geregelt war u. a. auch, dass für Besucher der Erhebungsstelle, die sich im Wege einer Beratung an diese wenden, ein separater Raum oder Bereich eingerichtet werden sollte, um die Vertraulichkeit zu wahren. Auch hier gab es die verschiedensten Lösungsansätze mit Besucherzonen, eigenen Wartezimmern oder speziellen Besprechungsräumen. Eine der Erkenntnisse des Zensus 2011 ist, dass Publikumsverkehr kaum stattgefunden hat, insoweit die bereitgestellten Ressourcen so gut wie nicht genutzt wurden. In der größten hessischen Stadt Frankfurt waren es nach Auskunft der Erhebungsstellenleitung keine zwei Dutzend Bürgerinnen oder Bürger, welche die Erhebungsstelle aufsuchten. Diese Erkenntnis trifft grundsätzlich für ganz Hessen zu. Einzige Ausnahme war der ländliche Vogelsbergkreis. Dort nutzten nach Angaben der Erhebungsstellenleitung etwa 300 Auskunftspflichtige das Beratungsangebot vor Ort.

3.7.2.1.9
Technik

Bei der Prüfung der technischen Umsetzung aller Vorgaben haben sich im Laufe der Zeit bestimmte Schwerpunkte heraus kristallisiert, die aus meiner Sicht besonders wichtig waren, weil sie entweder zu kritischen Sicherheitslücken führen könnten oder aber bei vielen Erhebungsstellen nicht zufriedenstellend gelöst waren.

3.7.2.1.9.1
Software-Umfang

So musste ich bis auf zwei alle Erhebungsstellen auffordern, die Software-Installation der Zensus-PC auf die vom HSL vorgesehenen Funktionalitäten zu begrenzen. In einigen Erhebungsstellen stellte das über die vorgesehenen Funktionalitäten hinausgehende Mehr an Software zwar keine unmittelbare Bedrohung für die geforderte Sicherheit dar. In anderen Fällen jedoch war Software zu finden, deren Installation ausdrücklich nicht auf den Zensus-Rechnern zur Verfügung stehen sollte (wie z. B. ein E-Mail-Client), damit die geforderte Trennung zum allgemeinen kommunalen Netz auch für die weitere Dauer des Erhebungsstellenbetriebs nicht gefährdet ist.

3.7.2.1.9.2
Zugriffe vom Zensus-Rechner ins Internet

An einigen Prüfungsergebnissen wurde deutlich, dass sich trotz richtiger Konzeption während der Betriebsphase an der einen oder anderen Stelle Fehler einschleichen konnten. In einem Fall war ein wichtiger Proxy-Server einige Zeit vor dem Prüfungstermin neu eingerichtet worden. Eigentlich sollten seine Einstellungen den Zugriff vom Zensus-PC ins Internet unterbinden. Durch diese Vorgabe sollte jegliches Risiko eines unbefugten Zugriffs auf die Zensus-Daten über das Internet ausgeschlossen werden. Bei der Neu-Installation waren diese, für den Erhebungsstellenbetrieb wichtigen Zusatzeinstellungen am Proxy-Server unterblieben. Bis zum Besuch meiner Mitarbeiter war dieses Problem offensichtlich Niemandem aufgefallen und somit waren die unzulässigen Zugriffe möglich. Nach einer Recherche der zuständigen Fachabteilung war klar, wie es dazu kommen konnte und das Problem wurde noch während des Prüftermins abgestellt. Bei meinen Prüfungen gab es allerdings noch zwei weitere Erhebungsstellen, bei denen der Zugriff von den geprüften Zensus-Arbeitsplätzen ins Internet möglich war. Ich habe mit Unterstützung des HSL darauf hingewirkt, dass diese Mängel umgehend behoben wurden.

3.7.2.1.9.3
Zugriffe auf das Intranet

Ein Gesichtspunkt, der im Vorfeld gar nicht betrachtet worden war, fiel erst zu Beginn der Prüfserie auf. Einer meiner Mitarbeiter stieß auf einen Listeneintrag unter den Favoriten des Browsers, der auf das kommunale Intranet zeigte. Wie sich bei der näheren Betrachtung ergab, war es zwar nicht möglich, einen anderen Bereich des lokalen Netzwerkes im Browser zu adressieren, aber das Intranet war in vollem Umfang zugänglich. Häufig wird das Intranet lediglich zur Verteilung verschiedenster Informationen genutzt und könnte daher als unproblematisch angesehen werden.

Im angesprochenen Fall beinhaltete das Intranet-Angebot aber auch eine Form von Softwareverteilung. Mitarbeiter, die dort hinterlegte Software-Tools für ihre Arbeit benötigten, konnten diese direkt auf ihr System übertragen und, da keine besonderen Rechte dafür nötig waren, selbst installieren. Da ein Zugriff auf das Intranet folglich mit unüberschaubaren zusätzlichen Risiken für die bewusst sehr restriktiv eingerichtete Arbeitsumgebung der Zensus-Rechner verbunden ist, habe ich im weiteren Verlauf der Prüfserie darauf geachtet, dass neben dem Internet auch keine Zugriffe auf das lokale Intranet möglich sind. Bei insgesamt 12 Erhebungsstellen musste daraufhin der Zugriff auf das Intranet unterbunden werden.

3.7.2.1.9.4
Erreichbarkeit des zentralen Zensus-Portals von nicht Zensus-Rechnern

Neben den Zensus-Rechnern standen den Mitarbeitern der Erhebungsstellen für den Austausch und die Bearbeitung von E-Mails und andere zulässige Zwecke in aller Regel weitere Arbeitsplatzrechner zur Verfügung, auf denen keine Daten des Zensus verarbeitet werden sollten und die demzufolge keinen Zugriff zum Portal haben durften. Leider ergaben die Prüfungen, dass in zwei Erhebungsstellen diese Grundforderung nicht umgesetzt war. In einem Fall ergeben sich bei meinen Mitarbeitern Zweifel, ob nicht sogar vorsätzlich entgegen der Vorgaben des HSL der Zugriff auf das Portal eingerichtet wurde. Auch wenn diese Mängel unmittelbar beseitigt wurden, müssen die Verantwortlichen in diesen Fällen mit einem erneuten Prüfbesuch rechnen.

3.7.2.1.9.5
Netztechnik

Um die Zensusrechner sicher gegen unbefugte Zugriffe aus den kommunalen Netzen zu schützen, sollte eine technische Trennung von der allgemeinen Verwaltung herbeigeführt werden. In einigen Erhebungsstellen wurden dazu die Zensus-Funktionalitäten durch eine Terminalserver-Sitzung realisiert. Diese wird so installiert, dass zwischen dem lokalen System und dem sogenannten Session-Client keine Daten ausgetauscht werden können. Idealerweise werden bei dieser Lösung die Zugriffe auf das Portal im lokalen Netz nur über den Terminalserver zugelassen.

Mit dieser technischen Lösung – eine beispielhafte Umsetzung fand sich bei der Stadt Frankfurt – haben einige Träger der Erhebungsstellen sehr elegant einerseits die gebotene Trennung realisiert und anderseits mit nur einem lokalen System eine vollständige Arbeitsumgebung einrichten können.

Daneben gab es sehr unterschiedliche Lösungsansätze für die Umsetzung des Trennungsgebots, die im Einzelfall das Spektrum von „gerade noch tolerierbar“ bis „sehr gut“ abdeckten. Insgesamt war hier die Umsetzung im Vogelsbergkreis besonders zu loben, der ein alle Einzelfragen umfassendes Gesamtkonzept vorbildlich umgesetzt hat.

3.7.2.1.9.6
Sperrung der CD/DVD-Laufwerke und USB-Anschlüsse

Um Veränderungen an den Zensus-Rechnern auszuschließen und um eine unbefugte Übertragung von Daten auf andere Datenträger zu verhindern,

war der Zugriff auf CD/DVD-Laufwerke und USB-Ports mit der Einrichtung der Systeme entsprechend einzuschränken. Während sich die Laufwerke, soweit keine Software-Lösung zur Verfügung steht, relativ leicht über passwortgeschützte BIOS-Einstellungen abschalten lassen, wurden in vielen Erhebungsstellen die Zugriffe auf die USB-Schnittstelle durch einen Eintrag in der Registry unterbunden.

Erfreulicherweise war festzustellen, dass viele Kreise und Städte bereits moderne Tools zur Steuerung der Schnittstellenzugriffe einsetzen und dadurch in der Lage sind, differenziert auf anfallende Anforderungen einzugehen. Dennoch musste ich auch in diesem Bereich in acht Fällen zur Nachbesserung auffordern.

3.7.2.1.9.7
Regelungen des Passwortgebrauchs

Erschreckend waren die Prüfungserkenntnisse im Bereich der Passwortregeln. Obwohl ich seit vielen Jahren bei meinen Prüfungen und in meinen Berichten immer wieder darauf hinweise, dass bei der Gestaltung der Passwortregeln die Standards aus den Maßnahmenkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umzusetzen sind, gibt es hier immer noch Defizite.

So hatten mehrere Kommunen nur 6-stellige, eine sogar nur 5-stellige Passwörter als Mindestlänge vorgegeben. Ich habe darauf gedrängt, dass dies im Bereich der betroffenen Erhebungsstellen sofort geändert wurde. Die jeweiligen Städte und Kreise sind generell aufgefordert, ihre Systemeinstellungen an die im Maßnahmenkatalog 2.11 des BSI beschriebenen Vorgaben anzupassen (www.bsi.bund.de).

3.7.2.1.9.8
Verpflichtung der beteiligten DV-Mitarbeiter auf das Statistikgeheimnis

Insgesamt zeigten alle Beteiligten, die für die technische Umsetzung an den Arbeitsplätzen und den kommunalen Netzen verantwortlich sind, bei allem Aufwand durchaus Verständnis für die besonderen Ansprüche bei Einrichtung und Betrieb der Erhebungsstellen. Mängel wurden soweit möglich noch am Tag der Prüfung abgestellt. In vielen Fällen jedoch fehlte den Beteiligten die Kenntnis der gesetzlichen Grundlagen. Entgegen der sonst üblichen Abgrenzung verschiedener Aufgabenbereiche innerhalb der Kommunalverwaltung fordert das Zensusausführungsgesetz deutlich schärfer eine Trennung von der sonstigen kommunalen Verwaltung.

Um bei dem betroffenen Personenkreis diesen Aspekt stärker ins Bewusstsein zu rücken und andererseits eine Kenntnisnahme von Zensus-Daten im Zusammenhang mit Service-Leistungen der DV-Mitarbeiter besser abzusichern, habe ich dem HSL vorgeschlagen, diese Mitarbeiter-Gruppe, soweit das in einzelnen Kommunen nicht bereits geschehen war, wie alle anderen Beteiligten förmlich auf das Statistik-Geheimnis zu verpflichten. Dies ist umgehend erfolgt.

3.7.2.1.10
Fazit

Die Ergebnisse meiner Überprüfungen in den Erhebungsstellen haben keine Mängel deutlich werden lassen, welche die praktische Ausführung des Zensus insgesamt oder die Handhabung in den einzelnen Erhebungsstellen hätten in Frage stellen müssen. Gleichwohl gab es durchaus markante Unterschiede, was Umfang und inhaltliche Qualität vorhandener Defizite anbelangt. Unverschlossene Türen, fehlende Verpflichtungserklärungen, Zugang vom Zensus-PC ins Internet oder das hauseigene Intranet, um nur einige zu nennen; eigentlich blieb keine Erhebungsstelle vollkommen ohne Fehl und Tadel. Dennoch bleibt festzustellen, dass das eingesetzte Personal trotz aller Fehleinschätzungen hinsichtlich des Arbeitsanfalls und der zeitlichen und organisatorischen Dimension des Unternehmens ‚Zensus 2011', hoch motiviert und kompetent die große Arbeitsbelastung bewältigt hat.

3.7.2.2
Auftragsdatenverarbeitung

Bereits im Frühjahr 2010 wurden einige Datenschutzbeauftragte mit der Frage nach der Zulässigkeit einer Auftragsdatenverarbeitung konfrontiert. Die Bundesländer Hessen, Sachsen und Sachsen-Anhalt beabsichtigten, den Versand und die Erfassung der ausgefüllten Bögen der Gebäude- und Wohnungszählung (GWZ) sowie der Haushaltsbefragung durch externe private Dienstleister abwickeln zu lassen. Thüringen beschränkt sich auf den Versand der Unterlagen der GWZ durch ein privates Unternehmen. So entstand eine grundsätzliche Diskussion unter den Datenschützern, ob eine derartige Beauftragung statistikrechtlich zulässig sei. Meine Rechtsauffassung hierzu habe ich frühzeitig geäußert und auch im 39. Tätigkeitsbericht (Ziff. 3.3.4) dargelegt. Danach konnte das HSL externe Dienstleister beauftragen, ohne damit gegen Vorschriften der Statistikgesetze oder des HDSG zu verstoßen. Mit den jeweiligen Unternehmen musste jedoch ein Vertrag

über die Datenverarbeitung im Auftrag abgeschlossen werden. Hierin waren u. a. meine Kontrollbefugnisse bei den privaten Dienstleistern zu sichern. Diese Forderungen wurden erfüllt.

3.7.2.2.1
Versand der Erhebungsbögen der Gebäude- und Wohnungszählung

Der Versand der Erhebungsunterlagen der GWZ erfolgte durch ein Tochterunternehmen des Deutschen Post AG mit Sitz in Einbeck in Niedersachsen. Um eine sog. „Personalisierung“ der Bögen vornehmen zu können, mussten die Anschriften der 2,4 Millionen hessischen Gebäude- und Wohnungseigentümer vom HSL an das Unternehmen übermittelt und dort in einem komplexen Arbeitsprozess auf die Bögen aufgedruckt werden. Für die Datenspeicherung im Rechenzentrum wurde ein eigener Server installiert, der mittels einer externen Festplatte auf die hessischen Daten zugreifen konnte. Auch die Länder Thüringen, Sachsen, Sachsen-Anhalt und Rheinland-Pfalz bedienten sich dieses Dienstleisters und des Verfahrens. Sicherzustellen war, dass die Daten getrennt von den übrigen Datenbeständen des Unternehmens gespeichert und weiterverarbeitet wurden. Meine Mitarbeiter haben das Verfahren insgesamt dreimal in Einbeck kontrolliert und an bestimmten Stellen Nachbesserungen, insbesondere hinsichtlich der Protokollierung, eingefordert.

3.7.2.2.2
Erfassung der Bögen der GWZ und Haushaltsbefragung

Für diese Form der Auftragsdatenverarbeitung wurde ein Unternehmen mit Sitz in Hallstadt (bei Bamberg) beauftragt, das meinen Mitarbeitern bereits im Zusammenhang mit der Verarbeitung von medizinischen Daten bekannt war. Das Unternehmen wurde ebenfalls dreimal kontrolliert. Hinzu kam in zwei Fällen die Inaugenscheinnahme eines Unterauftragnehmers in Bamberg, der in Spitzenzeiten Erfassungsdienstleistungen mit übernahm sowie ein Besuch bei einem Dienstleister in Pulsnitz (bei Dresden), der Bögen der GWZ im Unterauftrag bearbeitete. Auch bei diesen Dienstleistern gab es keinen Anlass zur Intervention. Alle Unternehmen, die als Tochterunternehmen der Schweizer Post tätig sind, wickelten den Auftrag ordnungsgemäß ab, wie ich zum Zeitpunkt meiner Prüfungen feststellen konnte. Auch hier gab es nur wenige Punkte zu bemängeln, die jedoch schnell behoben wurden. So war z. B beim Dienstleister in Hallstadt der Zutritt zum Serverraum einem unverhältnismäßig großen Personenkreis gestattet. Auch bei der Protokollierung kam es nach meinen Kontrollbesuchen zu Ergänzungen. Die

Beauftragung von Unterauftragnehmern wurde vertraglich abgesichert und war mit dem HSL sowie meinem Haus abgestimmt. Auch bei den Unterauftragnehmern waren keine Mängel in der Ablauforganisation feststellbar.

3.7.2.2.3
Was passiert mit den personenbezogenen Daten?

Diese Frage steht am Ende eines jeden Datenverarbeitungsprozesses. Nach § 19 ZensusG sind die Hilfsmerkmale von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren und spätestens vier Jahre nach dem Berichtszeitpunkt zu löschen. Die Erhebungsunterlagen sind nach Abschluss der Aufbereitung des Zensus, spätestens vier Jahre nach dem Berichtszeitpunkt zu löschen.

Diese Fristen gelten hinsichtlich der externen Dienstleister nur bedingt. Zunächst ist hier das Unternehmen in Einbeck zu nennen, an welches weit mehr als zwei Millionen Adressdaten von Gebäude- und Wohnungseigentümern übermittelt wurden. Hinzu kommt das Mahnverfahren, das ebenfalls über Einbeck abgewickelt werden sollte. Die Daten sind hilfsweise an einen Dritten für einen bestimmten Teil der Erhebungsorganisation (dem Versand der Unterlagen) übermittelt und dort gespeichert worden. In diesem Fall gilt die Regelung des frühestmöglichen Zeitpunkts der Löschung, d. h. zeitnah nach der Abwicklung des Versands der Erhebungsbögen sind die Daten zu löschen bzw. die Datenträger zu vernichten. Die Adressdaten auf den eigens hierfür angeschafften Platten und der Sicherungsmedien werden demnach nach Abschluss des Mahnverfahrens gelöscht bzw. die Festplatten datenschutzgerecht unter der Kontrolle der Auftraggeber entsorgt. Die Daten bei dem externen Dienstleister ‚Erfassung‘ unterliegen grundsätzlich den gleichen Bedingungen, könnten jedoch in Bezug auf die Erhebungspapiere bis zur vier Jahre nach dem 9. Mai 2011 (Stichtag) gespeichert bzw. gelagert werden. Selbstverständlich haben hieran weder die amtliche Statistik noch der Dienstleister ein Interesse. Derzeit werden die Erhebungsbögen der GWZ sowie der Haushaltsbefragung der Bundesländer Hessen, Sachsen und Sachsen-Anhalt bei dem Unterauftragnehmer in Bamberg gelagert. Die ursprüngliche vorgesehene rollierende Vernichtung der Bögen ist derzeit ausgesetzt, weil die Übernahme der Dateien vom Auftragnehmer in die Datenbanken der Statistikämter zum Berichtszeitpunkt stockt. Nach Auskunft des HSL (Stand Januar 2012) wurde mit der Vernichtung der Erhebungsbögen Ende Dezember 2011 begonnen.

3.7.2.3
Zusammenarbeit mit dem Statistischen Landesamt

Grundsätzlich war die Zusammenarbeit mit den zuständigen Mitarbeitern des HSL kooperativ und vertrauensvoll. Insbesondere hinsichtlich der Auftragsdatenverarbeitung wurden meine Mitarbeiter stets aktuell unterrichtet. Alle notwendigen Unterlagen waren im Vorfeld vorhanden und dann, wenn dies nicht der Fall war, im Nachgang besorgt. So war es meinen Mitarbeitern möglich, diesen überaus komplexen und zunächst nicht unproblematischen Datenverarbeitungsprozess immer mitzubegleiten, um dann, wenn es erforderlich schien, zu intervenieren. Die durch das HSL eingerichtete zentrale Erhebungsstelle haben meine Mitarbeiter zunächst nur in Augenschein genommen. Eine formale Prüfung der Datenverarbeitung im Statistikamt steht noch aus.

3.7.2.4
Bürgereingaben

Die ersten Wochen nach dem Stichtag 9. Mai waren erwartungsgemäß arbeitsintensiv, was die Beantwortung mündlicher und schriftlicher Anfragen anbelangt. Insgesamt war das Protest- und Nachfragepotential jedoch überschaubar. Meine Mitarbeiter haben nach dem Stichtag etwa 700 Telefonate geführt und bislang etwa 100 Eingaben schriftlich beantwortet. In fast allen Fällen konnten aufgetretene Missverständnisse und Falschinformationen aufgeklärt werden. Etwas komplizierter verhielt es sich mit den Auskunftspflichtigen, denen unzutreffend Immobilien zugeordnet wurden oder die mehrfach Bögen erhielten. Dabei handelte es sich nicht um wenige Einzelfälle, sondern um eine Fülle von Betroffenen. Daraus kann gefolgert werden, dass die Qualität der herangezogenen Register offensichtlich zu wünschen übrig lässt. So musste in vielen Fällen eine Aufklärung vor Ort durch Erhebungsbeauftragte erfolgen. Eine Rückkopplung der Ermittlungen an die Register führenden Stellen ist jedoch nicht erlaubt (sog. Rückspielverbot).

Zusammenfassend ist festzustellen, dass die befürchteten, massiven Proteste im Großen und Ganzen ausgeblieben sind. Ohne Zweifel kam es im Zusammenhang mit der Abwicklung des Zensus in einzelnen Fällen zu Problemen. Nicht erfasste Bögen, eine Vielzahl zugestellter Erhebungsunterlagen für nicht vorhandene Immobilien im Rahmen der GWZ oder aber unzuverlässige Erhebungsbeauftragte bei der Haushaltsbefragung: so etwas gab es im Einzelfall. Dennoch handelt es sich hierbei im Vergleich zu dem Gesamtvolumen von mehr als 2,4 Millionen Gebäude- und Wohnungseigentümern, die angeschrieben wurden, und knapp 750.000 Einwohner, die im Rahmen der Haushaltsbefragung befragt wurden, um eine überaus geringe Quote.

3.7.2.5
Eine erste Bilanz

Das Unternehmen Volkszählung (Zensus) 2011 ist von seiner Abwicklung her unter datenschutzrechtlichen Fragestellungen gelungen. Wie nicht anders zu erwarten, kam es im Verlauf der einzelnen Phasen immer wieder einmal zu Beschwerden oder Nachfragen, denen meine Mitarbeitern nachgingen. Gravierende Verstöße gab es keine. Unzulänglichkeiten entsprangen dem Fehlverhalten einzelner Mitarbeiter oder hatten organisatorische Hintergründe. Diese Einschätzung gilt sowohl für die Erhebungsstellenorganisation, die Abwicklung der Gebäude- und Wohnungszählung als auch die Haushaltsbefragung. Die Beauftragung externer Dienstleister führte zu einer höheren Komplexität der Datenverarbeitungsprozesse und bedeutete für meine Mitarbeiter eines erhebliches Mehr an Aufwand. Dennoch gelang es, die Abwicklung auch in diesem Bereich stetig zu begleiten und auch zu kontrollieren.

Eine weiterführende Analyse und Bewertung des Verfahrens kann erst im nächsten Berichtszeitraum erfolgen. Dann wird sich der Fokus auf die Datenverarbeitung im HSL richten. Die Datenschutzbeauftragten des Bundes und der Länder beabsichtigen, ihre Erfahrungen zusammenzuführen und in einer Stellungnahme zu dokumentieren. Beim nächsten Zensus oder ähnlichen registergestützten Verfahren sollte auf ein solches Papier zurückgegriffen werden können, um ähnlich gelagerte Fehler, wie sie jetzt aufgetreten sind, von vorneherein ausschließen zu können.

3.8 Gesundheitswesen

3.8.1
Datenverarbeitung in Pflegestützpunkten

In Hessen werden in jedem Landkreis und jeder kreisfreien Stadt zur wohnortnahen Beratung, Versorgung und Betreuung Pflegestützpunkte eingerichtet. Da in den Pflegestützpunkten sehr sensitive Daten verarbeitet werden, hat meine Dienststelle den datenschutzrechtlichen Rahmen für die Tätigkeit der Pflegestützpunkte gemeinsam mit den beteiligten Stellen geklärt und ein Informationsblatt für die Betroffenen initiiert.

3.8.1.1
Einrichtung und Aufgaben der Pflegestützpunkte

Gem. § 92c Abs. 1 Sozialgesetzbuch (SGB) XI richten die Pflegekassen und Krankenkassen zur wohnortnahen Beratung, Versorgung und Betreuung der Versicherten Pflegestützpunkte ein, sofern die zuständige oberste Landesbehörde dies bestimmt. Im Landespflegeausschuss, in dem die Kostenträger, Leistungserbringer und Betroffenenverbände vertreten sind, hat sich die Landesregierung 2008 zur Einrichtung von Pflegestützpunkten entschieden. Zunächst soll in jedem Landkreis und jeder kreisfreien Stadt ein Pflegestützpunkt mit Pflegeberatung eingerichtet werden. In Hessen sind 26 Pflegestützpunkte geplant. Die Pflege- und Krankenkassen errichten die Pflegestützpunkte mit den örtlichen Trägern der Sozialhilfe in gemeinsamer Trägerschaft.

Die Aufgaben der Pflegestützpunkte sind in § 92c SGB XI detailliert festgelegt. Sie umfassen insbesondere die folgenden Punkte:

- Erhebung aller sozialen, gesundheitlichen und pflegerischen Versorgungs-, Betreuungs- und Beratungsangebote einschließlich der relevanten Aktivitäten der Selbsthilfe und des bürgerschaftlichen Engagements im Einzugsbereich des Pflegestützpunktes und Erstellen von entsprechenden Informationsunterlagen.
- Vernetzung aufeinander abgestimmter pflegerischer und sozialer Versorgungs-, Betreuungs- und Beratungsangebote.
- Abstimmung und Koordinierung der für die wohnortnahe Versorgung und Betreuung in Betracht kommenden gesundheitsfördernden, präventiven, kurativen, rehabilitativen und sonstigen medizinischen sowie pflegerischen und sozialen Hilfs- und Unterstützungsangebote.
- Information, Auskunft und Beratung für alle Bürgerinnen und Bürger ihres Einzugsbereiches. Die Pflegestützpunkte beraten zu Rechten und Pflichten nach dem Sozialgesetzbuch und zur Auswahl und Inanspruchnahme der bundes- oder landesrechtlich vorgesehenen Sozialleistungen und sonstigen Hilfsangebote.

3.8.1.2
Datenschutzrechtliche Vorgaben

Da von den Pflegestützpunkten sensitive Daten der Ratsuchenden verarbeitet werden, müssen die Rechtsgrundlagen sowie Umfang, Zweck und Dauer der Datenverarbeitung für die beteiligten Stellen und die Rat suchenden Bürgerinnen und Bürger klar und transparent sein. Meine Dienststelle hat daher gemeinsam mit dem Steuerungsausschuss Pflegestützpunkte

des Hessischen Städtetags die datenschutzrechtlichen Vorgaben und die künftigen Verfahrensweisen einschließlich eines Merkblatts für die Rat suchenden Bürgerinnen und Bürger geklärt.

3.8.1.2.1
Rechtsgrundlage für die Verarbeitung personenbezogener Daten

§ 92c SGB XI ist eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Pflegestützpunkt, soweit die Verarbeitung der Daten für die Aufgabenerfüllung des Pflegestützpunkts erforderlich ist. Es handelt sich bei dieser Vorschrift sowohl um eine Aufgaben- wie auch um eine Befugnisnorm.

§ 92c SGB XI

... Im Pflegestützpunkt tätige Personen ... dürfen Sozialdaten nur erheben, verarbeiten und nutzen, soweit dies zur Erfüllung der Aufgaben nach diesem Buch erforderlich oder durch Rechtsvorschriften des Sozialgesetzbuchs ... angeordnet oder erlaubt ist.

Darüber hinaus ist in § 4 SGB XII (Sozialhilfe) die Tätigkeit der Träger von Sozialleistungen geregelt.

§ 4 SGB XII

(1) .... Darüber hinaus sollen die Träger der Sozialhilfe gemeinsam mit den Beteiligten der Pflegestützpunkte nach § 92c SGB XI alle für die wohnortnahe Versorgung und Betreuung in Betracht kommenden Hilfe- und Unterstützungsangebote koordinieren.

...

(3) Soweit eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt, ist das Nähere in einer Vereinbarung zu regeln.

Da mit den o. a. Regelungen eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten in den Pflegestützpunkten vorliegt, bedarf es nicht zusätzlich einer gesonderten datenschutzrechtlichen Einwilligung der Betroffenen in die Verarbeitung ihrer Daten.

3.8.1.2.2
Transparenz für die Betroffenen

Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die vom Pflegestützpunkt vorgenommene Verarbeitung personenbezogener Daten für die Betroffenen transparent ist. Gefordert wurde von meiner Dienststelle, dass Transparenz der Datenverarbeitung durch ein Merkblatt

sichergestellt wird, das im Pflegestützpunkt für jeden Ratsuchenden zur Verfügung steht und über die wesentlichen Aspekte der Datenverarbeitung informiert. Dieses Merkblatt wurde inzwischen mit meiner Beratung erarbeitet und steht in den Pflegestützpunkten für die Betroffenen zur Verfügung. Darüber hinaus steht den Betroffenen gem. § 83 SGB X ein Auskunftsrecht gegenüber dem Pflegestützpunkt zu, auf das in dem Merkblatt hingewiesen wird.

§ 83 SGB X

Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. *die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,*
2. *die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und*
3. *den Zweck der Speicherung.*

Für die Pflegestützpunkte empfiehlt es sich, wesentliche Ergebnisse des Beratungsgesprächs das weitere Tätigwerden des Pflegestützpunkts betreffend schriftlich zu dokumentieren. Als Akzeptanz fördernde Maßnahme kann den Betroffenen z. B. zusätzlich die Aushändigung eines Ausdrucks des im Pflegestützpunkt gespeicherten Datensatzes bzw. der Besprechungsergebnisse angeboten werden. Eine solche Verfahrensweise ist vom Hessischen Städtetag befürwortet worden.

3.8.1.2.3
Umfang der erforderlichen Datenverarbeitung

In Hessen gibt es einen Rahmenvertrag des Hessischen Städtetags für Vereinbarungen zwischen den Pflegekassen und den Städten. Die darin enthaltenen Vereinbarungen zur Verarbeitung personenbezogener Daten bedürfen aber der Konkretisierung.

Der Gesetzgeber hat den Pflegestützpunkten komplexe Aufgaben zugewiesen, die im Einzelfall mit der Verarbeitung umfangreicher sensitiver Daten verbunden sein können. Für diesen Zweck wird von den Pflegestützpunkten in Hessen – wie auch in einer Reihe weiterer Bundesländer – die Software synCASE eingesetzt. Diese Software ermöglicht z. B. die generelle Erfassung der für die Pflegestützpunkte relevanten ambulanten Pflegedienste, Ämter, Apotheken, Ärzte, Heilmittelerbringer, Sanitätshäuser, teilstationären und stationären Einrichtungen sowie der Kostenträger und darüber hinaus unter Anderem im Rahmen der Fallaufnahme und Beratung die Erfassung detaillierter Daten über die Betroffenen – etwa zu ihren bisher beantragten/erhaltenen Versicherungsleistungen, der erfolgten Pflegebe-

gutachtung, Behinderungen, Krankheiten, der Wohnsituation und dem Umfang des momentanem Hilfebedarfs. Bei der Nutzung dieser Software ist zu beachten, dass personenbezogene Daten im Pflegestützpunkt nur in dem für die Aufgabenerfüllung erforderlichen Umfang verarbeitet werden dürfen. Das heißt insbesondere:

- Soweit es nur um punktuelle Informationsanfragen geht, z. B. welche Anbieter es für bestimmte Leistungen gibt, oder um die Bitte um Zusendung von Informationsmaterial (z. B. Listen von Pflegedienstadressen) oder vergleichbare Informationsanfragen, ist eine Speicherung der personenbezogenen Daten der Betroffenen nach der Beantwortung der Anfrage nicht mehr erforderlich und damit nicht zulässig. Auch bei kurzen Beratungen, insbesondere, wenn die Betroffenen keine Datenverarbeitung wünschen, wird regelmäßig auf personenbezogene Datenspeicherungen verzichtet werden können. Die Software sieht die Möglichkeit der Erfassung einer Beratung unter einer anonymen Beratungsnummer vor und – soweit überhaupt eine Datenerfassung als notwendig angesehen wird – muss diese Möglichkeit in diesen Fällen auch genutzt werden.
- Soweit es um die Vermittlung z. B. eines speziellen Pflegedienstes geht und z. B. vom Pflegestützpunkt spätere Nachfragen beim Betroffenen vorgesehen sind, ob die Versorgung passend und ausreichend ist, ist eine Speicherung der Daten der Betroffenen im erforderlichen Umfang zulässig. Aus fachlicher Sicht zählt es zu den Aufgaben der Pflegestützpunkte, dass Hilfe soweit notwendig gesichert wird.
- Soweit im Pflegestützpunkt erforderliche Hilfen koordiniert werden und ein Versorgungsplan für den Betroffenen erstellt wird, ist ebenfalls eine Verarbeitung der Daten des Betroffenen im erforderlichen Umfang zulässig. Dies kann z. B. auch detaillierte medizinische Daten und Daten über den aktuellen Hilfebedarf beinhalten.

Die Aufgabenerfüllung kann im Einzelfall auch die Übermittlung von Daten vom Pflegestützpunkt an die zuständige Pflegekasse oder das zuständige Sozialamt oder z. B. an einen Pflegedienst einschließen oder umgekehrt die Übermittlung der zuständigen Pflegekasse oder des zuständigen Sozialamts an den Pflegestützpunkt.

3.8.1.2.4
Ausgestaltung der Zugriffsmöglichkeiten auf den Datenbestand im Pflegestützpunkt

Im Pflegestützpunkt arbeiten sowohl Mitarbeiter des örtlichen Sozialhilfeträgers, die bei Bedarf einen evtl. Rechtsanspruch auf eine Sozialleistung

(z. B. Übernahme der Kosten für den Pflegedienst) klären, als auch Mitarbeiter einer Pflegekasse, die die Betroffenen hinsichtlich einer evtl. erforderlichen passgenauen Pflegeleistung berät und diese auch bei Bedarf koordiniert. Die Mitarbeiter der Pflegekassen werden in jedem Pflegestützpunkt jeweils beratend tätig für alle Pflegekassen in Hessen. Da nach fachlicher Einschätzung in den meisten Beratungen beide Fragenbereiche eine Rolle spielen (können), wurde eine Zugriffsdifferenzierung innerhalb des Pflegestützpunkts fachlich als nicht möglich angesehen. Sie ist daher auch datenschutzrechtlich nicht geboten.

3.8.1.2.5
Abschottung des Datenbestands des Pflegestützpunkts vom örtlichen Sozialhilfeträger und von den Pflegekassen

Der Datenbestand des Pflegestützpunkts ist grundsätzlich sowohl vom örtlichen Sozialhilfeträger wie auch von den Pflegekassen abzuschotten. Der Pflegestützpunkt ist eine eigenständige, im SGB XI gesetzlich geregelte Stelle, d. h. insbesondere, dass der Träger vor Ort nicht die Möglichkeit haben darf, auf den Datenbestand des Pflegestützpunkts zuzugreifen. Umgekehrt darf ein Mitarbeiter des Pflegestützpunkts nicht die Möglichkeit haben, auf den Datenbestand des örtlichen Sozialhilfeträgers direkt zuzugreifen. Soweit im Einzelfall für die Aufgabenerfüllung im Pflegestützpunkt ergänzende Informationen aus dem Datenbestand des örtlichen Sozialhilfeträgers benötigt werden, können diese über einen Mitarbeiter des örtlichen Sozialhilfeträgers erhoben werden. Entsprechendes gilt für den Datenbestand der Pflegekassen.

3.8.1.2.6
Grundsatz der Datensparsamkeit

Darüber hinaus muss sichergestellt werden, dass nicht künftig alle an einer Beratung und Koordination beteiligten Stellen – Pflegestützpunkt, örtlicher Sozialhilfeträger, im Pflegestützpunkt beratende Pflegekasse, für den Betroffenen zuständige Pflegekasse, kontaktierter Pflegedienst – pauschal einen umfassenden Datenbestand über einen Betroffenen speichern. Vielmehr ist es dringend geboten, dass die beteiligten Stellen ihre jeweiligen Aufgaben und die von ihnen hierfür benötigen Daten im Beratungs- und Koordinationsprozess klar abgrenzen. Seitens des Datenschutzes kann diese Aufgabenabgrenzung nicht vorgenommen werden, sie ist eine fachliche Entscheidung. Seitens des Datenschutzes kann und muss aber gefordert werden, dass eine solche klare Aufgabenabgrenzung erfolgt und auch für die Betroffenen transparent wird.

3.8.1.2.7
Dauer der Datenspeicherung

Eine Speicherung der Daten der Ratsuchenden darf nur solange erfolgen, wie dies zur Aufgabenerfüllung des Pflegestützpunkts erforderlich ist.

> *§ 84 Abs. 2 SGB X*
>
> *Sozialdaten sind zu löschen, wenn ihre Speicherung unzulässig ist. Sie sind auch zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden.*

Soweit eine personenbezogene Datenverarbeitung im Pflegestützpunkt vorgenommen wird, sollte die Dauer der Speicherung der Daten geklärt und in dem Merkblatt erläutert werden. Die Gespräche mit dem Städtetag und mit einzelnen Pflegestützpunkten haben ergeben, dass die Daten in der Regel spätestens nach Ablauf von drei Jahren nach dem letzten Kontakt mit dem Betroffenen nicht mehr benötigt werden und daher gelöscht werden müssen.

Da die Pflegestützpunkte neu aufgebaut werden, können sich neue und zusätzliche datenschutzrechtliche Fragestellungen ergeben, die dann von meiner Dienststelle in Abstimmung insbesondere mit dem Hessischen Städtetag geklärt werden.

3.8.2
Datenschutzkonzepte für altersgerechte Assistenzsysteme

Auch in Hessen werden Projekte zum Einsatz intelligenter Assistenzsysteme für ein selbstbestimmtes Leben im Alter entwickelt. Bestandteil derartiger Projekte ist stets auch die Verarbeitung sensitiver Gesundheitsdaten durch mehrere Projektbeteiligte. Angemessene Datenschutzkonzepte müssen in die Ausgestaltung der Projekte von Anfang an einbezogen werden.

3.8.2.1
Ziele von AAL

Vor dem Hintergrund des demografischen Wandels werden seit einigen Jahren sog. AAL-(Ambient Assisted Living-)Projekte zunehmend diskutiert und entwickelt (siehe z. B. http://www.iat.eu/ehealth/). Es geht dabei um intelligente Assistenzsysteme für ein selbstbestimmtes, gesundes, unabhängiges Leben im eigenen Hause. An AAL-Technologien arbeiten viele Sparten, von der Medizin- über die Hausgeräte- und Kommunikations- bis

zur Mikrosystemtechnik. Dienstleistungen und technische Lösungen sollen so verbunden werden, dass ältere Menschen möglichst lange in der eigenen Wohnung leben können, z. B. mit Hilfe von neuartigen telemedizinischen Lösungen, mit technischen Helfern, die einen Teil der täglichen Hausarbeit übernehmen, mit Sensoren etwa an Türen, Teppichen oder Leuchten, die Bewegung und Verhalten registrieren und auswerten, um häusliche Unfälle zu verhindern (z. B. automatisches Anschalten der Beleuchtung bei Betreten eines Raumes) oder um Notfälle zu erkennen (z. B. RFID-Chips im Teppich, die den genauen Aufenthalt in der Wohnung registrieren und ggfs. eine Information an die Rettungsleitstelle auslösen), oder auch mit intuitiv bedienbaren Kommunikationsmitteln, die den Kontakt mit dem sozialen Umfeld erleichtern. Das Bundesministerium für Bildung und Forschung (BMBF) fördert seit 2008 Projekte im Bereich AAL (http://www.aal-deutschland.de/deutschland).

3.8.2.2
Datenschutzrechtliche Aspekte

Es liegt auf der Hand, dass bei derartigen Projekten auch immer sensitive Daten der Betroffenen verarbeitet werden. Bei umfassenden Projekten sind die Gefahren einer Profilbildung zu beachten und die Vielzahl von beteiligten Stellen, Systemen und Datenübermittlungen machen es schwer, für die Betroffenen Transparenz herzustellen und die Wahrnehmung ihrer Rechte sicherzustellen.

Zunächst entstehen Daten in der Wohnung bzw. am Körper der Betroffenen, diese werden dann je nach Projektinhalt unter bestimmten Voraussetzungen an externe Stellen weitergeleitet. Rechtsgrundlage hierfür ist in der Regel ein Vertrag mit dem Betroffenen, für den der 4. Abschnitt des BDSG (§§ 27 ff.) zu beachten ist. Für die Projektteilnehmer muss bei Vertragsabschluss Umfang und Art und Weise der Verarbeitung ihrer personenbezogenen Daten – die teilweise als „besondere Arten personenbezogener Daten“ i. S. v. § 3 Abs. 9 BDSG verschärften datenschutzrechtlichen Vorgaben unterliegen – transparent sein, d. h. ihnen muss in jedem Fall eine verständliche schriftliche Information zur Verarbeitung ihrer Daten ausgehändigt werden. Bei umfangreicheren komplexen Projekten ist eine gesonderte Einwilligung der Betroffenen in die Verarbeitung ihrer Daten i. S. v. § 4a BDSG zu fordern. Je nach Projektinhalt sollten die entstehenden Daten möglichst erst dann an externe Stellen weitergeleitet werden, wenn Handlungsbedarf besteht, und auch nur im jeweils erforderlichen Umfang. Die Betroffenen sollten so umfassend und so lange wie möglich die Verfügungsmacht über ihre Daten behalten. Bei dem gesamten Projekt

sollte der Grundsatz der Datensparsamkeit beachtet werden. Der Projektteilnehmer hat ein Recht auf Auskunft gem. § 34 BDSG und Rechte auf Widerspruch, Löschung oder Sperrung nach § 35 BDSG. Diese Rechte können ggfs. auch durch den gesetzlichen oder den gewillkürten Vertreter oder auch durch einen Betreuer wahrgenommen werden. Da es sich regelmäßig um Verbundprojekte handelt, ist die eindeutige Klärung und verbindliche Festlegung der jeweiligen Verantwortlichkeit für Datenschutz und Datensicherheit besonders wichtig. Angemessene technisch-organisatorische Datensicherheitsmaßnahmen müssen getroffen werden (z. B. Verschlüsselung der Gesundheitsdaten auf den zentralen Systemen und bei der Übertragung). Die in den Projekten involvierten Informations- und Kommunikationsdiensteanbieter müssen die Bestimmungen des Telekommunikationsgesetzes und des Telemediengesetzes beachten.

3.8.2.3
Projekte in Hessen

Auch in Hessen werden AAL-Projekte geplant bzw. entwickelt und getestet. Meine Dienststelle berät hinsichtlich der datenschutzrechtlichen Ausgestaltung. Im Berichtszeitraum habe ich insbesondere die Entwicklung des vom BMBF geförderten Projekts WohnSelbst (http://www.wohnselbst.de/) begleitet, das die HSK Rhein-Main GmbH (eine Management Holding Gesellschaft, zu der auch die Dr. Horst-Schmidt-Kliniken GmbH gehört) als Konsortialführer zusammen mit einer Wiesbadener Wohnungsbaugesellschaft und weiteren Partnerfirmen aus dem technischen Bereich bis 2012 betreibt. Erprobt werden soll insbesondere, inwieweit eine telemedizinische Betreuung chronisch kranke Menschen wirksam unterstützen kann und z. B. Krankenhausaufenthalte vermieden werden können. Die Wohnungen der Projektteilnehmer werden mit einem sog. Smart Living Manager ausgestattet, einer speziellen Steuerungseinheit des Fernsehgeräts, das über eine Serviceplattform via Internet mit einem medizinischen Betreuungscenter verbunden ist. Zu Beginn der Teilnahme an dem Projekt wird ein Gesundheitscheck durchgeführt. Den Projektteilnehmern werden dann bei Bedarf je nach Indikation medizinische Messgeräte zur täglichen Messung des Gewichts, des Blutdrucks und/oder des Blutzuckers zur Verfügung gestellt. Die aktuellen Vitalwerte werden elektronisch übertragen und bei auffälligen Werten werden zuvor mit dem Teilnehmer abgestimmte Maßnahmen getroffen, z. B. ein Anruf des medizinischen Betreuungscenters beim Betroffenen. Die Holding hat mich frühzeitig in die Diskussion der Ausgestaltung des Projekts einbezogen. Klärungsbedürftig waren insbesondere die folgenden Fragen:

– Welche der beteiligten Stellen hat welche Aufgabe in dem Projekt und in welchem Umfang und auf welche Art und Weise muss die jeweilige Stelle für ihre Aufgabe personenbezogene Daten der Teilnehmer erhalten? Wie lange müssen die Daten gespeichert werden? Wer benötigt darüber hinaus einen Zugriff auf diese Daten?

  Es handelt sich hier – wie bei fast allen AAL-Projekten – um ein Verbundprojekt. Die für das Projekt notwendigen Datenflüsse wurden intensiv diskutiert und in der Projektbeschreibung konkretisiert.
– Wie kann für die Teilnehmer Transparenz hinsichtlich der zu ihrer Person im Rahmen des Projekts durch verschiedene Stellen verarbeiteten Daten, insbesondere der medizinischen Daten, sichergestellt werden ?

  In die schriftliche Information der Projektteilnehmer über die Verarbeitung ihrer personenbezogenen Daten werden die grundlegenden Datenflüsse aufgenommen.
– Auf welche Weise können die Teilnehmer selbst Zugang zu ihren Daten haben?
– Welche technisch-organisatorischen Datensicherheitsmaßnahmen, insbesondere für die Datenübermittlung via Internet, sind erforderlich und ausreichend?
– Wann und wie werden die Daten derjenigen Personen, die ihre Teilnahme beenden, gelöscht bzw. vernichtet?

Die Holding hat die von mir in das Projekt eingebrachten datenschutzrechtlichen Aspekte umgehend aufgegriffen, konkretisiert und in die Teilnehmerunterlagen aufgenommen. Einige Details bleiben weiterhin diskussionsbedürftig, zumal das Projekt ständig weiterentwickelt wird.

Entsprechende Projekte werden auch weiterhin von meiner Dienststelle beraten. Mein zentrales Anliegen ist es dabei, die Projekte bei der datenschutzgerechten rechtlichen und technischen Ausgestaltung zu unterstützen.

3.8.3
Neue Orientierungshilfe für Krankenhäuser

Da die Umsetzung der datenschutzrechtlichen Anforderungen an die Zugriffsausgestaltung von Krankenhausinformationssystemen bundesweit Probleme aufwirft, haben die Datenschutzbeauftragten des Bundes und der Länder 2011 eine neue Orientierungshilfe „Krankenhausinformationssyteme“ veröffentlicht. Sie soll insbesondere Krankenhausträgern, Anwendern, Herstellern und internen Datenschutzbeauftragten eine detaillierte Orientierung ermöglichen.

3.8.3.1
Hintergrund

In meinen vorausgegangenen Tätigkeitsberichten habe ich ausführlich über die bundesweit existierenden Probleme hinsichtlich der Zugriffsausgestaltung in Krankenhausinformationssystemen berichtet (38. Tätigkeitsbericht, Ziff. 4.6.2; 39. Tätigkeitsbericht, Ziff. 4.7.1). Krankenhausinformationssysteme sind zu einem unverzichtbaren Hilfsmittel der Patientenbehandlung in Krankenhäusern geworden. Sie ermöglichen es, dass verschiedene Mitarbeiter des Krankenhauses jederzeit schnell und zeitgleich auf die elektronisch gespeicherten Patientendaten zugreifen können. Schnelle Information und Entscheidung wird dadurch möglich. Diese krankenhausweiten technischen Zugriffsmöglichkeiten machen andererseits aber auch eine differenzierte Regelung und Ausgestaltung der Zugriffsberechtigungen und eine Kontrolle ihrer Nutzung zwingend erforderlich. Eine Patientin bzw. ein Patient rechnet nicht damit und muss nicht damit rechnen, dass seine sensitiven detaillierten medizinischen Daten während seiner Behandlung – und möglicherweise sogar noch Jahre danach – jederzeit von allen – u. U. mehreren tausend – Mitarbeiterinnen und Mitarbeitern des Krankenhauses zur Kenntnis genommen werden können.

2008 hat der Europäische Gerichtshof für Menschenrechte (EGMR) sich erstmals mit der Ausgestaltung und Kontrolle von Krankhausdaten befasst und ebenfalls die Notwendigkeit von Zugriffsbegrenzung und Zugriffskontrolle hervorgehoben (s. 38. Tätigkeitsbericht, Ziff. 4.6.2.1.3).

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

Da in den letzten Jahren immer wieder bundesweit Probleme festgestellt wurden, hat nunmehr die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dieses Thema als Schwerpunktthema gewählt und 2011 eine neue Orientierungshilfe „Krankenhausinformationssysteme“ vorgelegt (s. Ziff. 9.1 und http://www.datenschutz.hessen.de/ft-gesundheit.htm). Sie wurde von einer Arbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz (UAG KIS) unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche erstellt. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinforma-

tionssystemen, Betreiber, Anwendervereinigungen und Datenschutzbeauftragte von Krankenhäusern einbezogen. Die Endfassung der Orientierungshilfe wurde 2011 zustimmend zur Kenntnis genommen von

- der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder,
- den obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich („Düsseldorfer Kreis“),
- den Datenschutzbeauftragten der EKD sowie
- der Konferenz der Datenschutzbeauftragten im Bereich der katholischen Kirche Deutschlands.

Der Wortlaut der Orientierungshilfe ist auf meiner Homepage veröffentlicht (http://www.datenschutz.hessen.de/ft-gesundheit.htm).

Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und für die internen Datenschutzbeauftragten von Krankenhäusern liegt damit ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb vor. Für die Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzaufsichtsbehörden wird das vorliegende Dokument den Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit bilden. Das Begleitpapier zur Orientierungshilfe führt hierzu Folgendes aus:

- Soweit sich die Anforderungen an die Krankenhäuser als Betreiber richten und entweder organisatorische Regelungen betreffen oder mittels vorhandener Informationstechnik umgesetzt werden können, soll die Orientierungshilfe bereits jetzt herangezogen werden.
- Mit Blick auf die Erfordernisse bei Softwareentwicklung und Qualitätssicherung gehen die Aufsichts- und Kontrollbehörden von der Notwendigkeit einer angemessenen Übergangsfrist für seitens der Hersteller erforderliche Anpassungen aus.

Inzwischen haben sich KIS-Hersteller bereits intensiv mit den in der Orientierungshilfe enthaltenen Forderungen und auch mit erforderlichen Anpassungen befasst.

Die Diskussion mit Herstellern und Betreibern von Krankenhausinformationssystemen hat gezeigt, dass technische Anforderungen, Strukturen und Prozesse im Krankenhausbetrieb einem dynamischen Wandel unterworfen sind. Die Aufsichts- und Kontrollbehörden werden daher zur Fortschreibung der Orientierungshilfe weiterhin den Dialog mit Herstellern, Betreibern und weiteren Experten suchen. Die UAG KIS hat 2011 auch mehrere Gespräche mit der Deutschen Krankenhausgesellschaft geführt.

Meine Dienststelle hat an der Erarbeitung der Orientierungshilfe mitgewirkt und u. a. mit der Hessischen Krankenhausgesellschaft und verschiedenen Kliniken ein Gespräch geführt über die künftige Umsetzung der Orientierungshilfe in Hessen.

3.8.3.2
Inhalt der Orientierungshilfe

Teil 1 der Orientierungshilfe „Normative Eckpunkte zur Zulässigkeit von Zugriffen auf elektronische Patientendaten im Krankenhaus“ konkretisiert die Anforderungen, die sich aus den derzeit bereits geltenden datenschutzrechtlichen Regelungen z. B. in Landeskrankenhausgesetzen, sowie den Vorgaben zur ärztlichen Schweigepflicht i. S. v. § 203 StGB und der Ärztlichen Berufsordnung ergeben. Zentrale Themenbereiche sind insbeson-dere

- Datenverarbeitung in der Aufnahme
- Datenverarbeitung während und im Rahmen der Behandlung
- Datenverarbeitung nach Abschluss der Behandlung
- Technische Administration
- Verarbeitung der Daten besonders schutzwürdiger Patientengruppen (z. B. VIPs, eigene Mitarbeiter des Krankenhauses)
- Zugriffsprotokollierung und Datenschutzkontrolle
- Auskunftsrechte des Patienten.

In Teil 2 „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen“ werden Maßnahmen zur technischen Umsetzung der rechtlichen Vorgaben beschrieben. Zentrale Themenbereiche sind insbesondere

- Systemfunktionen
- Anwendungsfunktionen
- Rollen- und Berechtigungskonzept
- Datenpräsentation
- Nutzungsergonomie
- Protokollierung
- Technischer Betrieb, Administration.

Als ersten Schritt müssen die Produkte bestimmte Funktionalitäten besitzen. Hier sind die Hersteller gefordert, im Klinikinformationssystem geeignete Funktionen und Mechanismen zur Verfügung zu stellen. Darauf aufbauend muss das System so konfiguriert werden, dass es im Betrieb die datenschutzrechtlichen Anforderungen berücksichtigt; dafür ist der Betreiber verantwortlich.

In der Orientierungshilfe wird daher nach Anforderung unterschieden, die sich an den Hersteller, den Betreiber oder beide richten. Außerdem findet eine Differenzierung nach dem Umsetzungserfordernis statt. Es gibt Muss- und Soll-Anforderungen und solche, die einen datenschutzfreundlichen Einsatz lediglich unterstützen. Da es nicht umgehend möglich ist, die technischen und organisatorischen Anforderungen umzusetzen, wird es insbesondere für eine Übergangszeit Systeme unterschiedlicher Güte geben. Um einheitliche Bewertungsmaßstäbe zu gewährleisten, beabsichtigen die Aufsichtsbehörden eine enge Abstimmung.

3.8.4
Verwendung für das Gesundheitsamt bestimmte medizinische Daten durch die Führerscheinstelle

Werden Tatsachen bekannt, die Bedenken gegen die körperliche oder geistige Eignung eines Führerscheininhabers begründen, kann die Fahrerlaubnisbehörde die Beibringung eines ärztlichen Gutachtens durch den Betroffenen anordnen. Die Verwendung von Informationen aus medizinischen Daten, die eigentlich für das Gesundheitsamt bestimmt waren, durch eine Führerscheinstelle zu Lasten eines Betroffenen ist dabei nicht ausgeschlossen.

3.8.4.1
Der Fall

Das Jobcenter des Wetteraukreises hatte einen Empfänger von Hartz IV-Leistungen hinsichtlich dessen Erwerbsfähigkeit untersuchen lassen. Einen entsprechenden Auftrag erhielt der Fachdienst Gesundheit und Gefahrenabwehr der Kreisverwaltung. Dieser setzte sich mit dem Betroffenen in Verbindung und ließ sich eine Entbindungserklärung von der Schweigepflicht für dessen Hausarzt und den Orthopäden unterzeichnen.

Im weiteren Verlauf des Verfahrens forderte der Fachdienst Gesundheit Befundberichte vom Hausarzt an, die dieser an die Kreisverwaltung übermittelte. Da die Unterlagen nicht als „vertraulich“ oder „Arztsache“ gekennzeichnet waren, öffnete die Posteingangsstelle den Umschlag. Bei deren Sichtung bzw. der Zuordnung kam man zu dem Schluss, dass diese Unterlagen für den Fachdienst Verkehr bestimmt sein müssten und leitete die medizinischen Berichte an die dort angesiedelte Führerscheinstelle weiter. Nach der Sichtung der Unterlagen, die der Fachdienst selbst nie angefordert hatte, kamen die zuständigen Bearbeiter dort zu dem Schluss, dass

berechtigte Zweifel an der Eignung des Betroffenen zur Führung eines Kraftfahrzeuges bestehen. Aus diesem Grund schrieb man diesen mit der Anordnung an, seine Eignung durch die Vorlage eines fachärztlichen Gutachtens mit Leistungstest nachzuweisen.

In einer Beschwerde bei meiner Dienststelle zweifelte der Betroffene die Zulässigkeit der Datenverwendung durch die Führerscheinstelle an. Er habe, so der Beschwerdeführer weiter, zwei ausdrücklich genannte Ärzte von der ärztlichen Schweigepflicht gegenüber dem Gesundheitsamt entbunden und müsse nun feststellen, dass die medizinischen Informationen zu seiner Person in belastender Weise von der Führerscheinstelle gegen ihn genutzt würden.

3.8.4.2
Rechtliche Beurteilung

In der Tat war es für den Beschwerdeführer überraschend, als er Post von der Führerscheinstelle und die Mitteilung erhielt, seine Fähigkeit zur Führung eines Kfz werde angezweifelt. Bislang stand er in Kontakt mit der JobKOMM GmbH des Kreises und dem Gesundheitsamt. Völlig unerwartet hatte er es plötzlich auch mit der Führerscheinstelle zu tun, die von ihm die Vorlage eines kostenpflichtigen medizinischen Gutachtens hinsichtlich seiner Fahrtauglichkeit verlangte. Nachvollziehbar zweifelte der Betroffene die Zulässigkeit der Verwendung seiner medizinischen Daten an und bat mich um eine rechtliche Bewertung.

Der Vorgang hatte verschiedene datenschutzrechtliche Facetten, die nachfolgend von mir zu bewerten waren:

3.8.4.2.1
Organisationsmängel innerhalb der Poststelle der Kreisverwaltung

Zu kritisieren war, dass das (wenn auch unzureichend adressierte) Gutachten des Hausarztes ohne vorherige Recherche hinsichtlich des genauen Adressaten, innerhalb der Kreisverwaltung von der Poststelle an den Fachdienst Verkehr weitergeleitet wurde. Hier hätte man zu Recht einen sensibleren Umgang mit den medizinischen Daten einfordern dürfen. Die Datenschutzbeauftragte des Wetteraukreises hat diesen Vorfall zum Anlass genommen, den Umgang mit personenbezogenen medizinischen Daten entsprechend deren Sensitivität neu zu regeln.

3.8.4.2.2
Unzureichende Adressierung der Unterlagen

Eine nicht unerhebliche Verantwortung für den Vorgang trägt der Hausarzt des Beschwerdeführers, bei dem die Unterlagen vom Fachdienst Gesundheit angefordert wurden. Eine korrekte Adressierung mit dem zusätzlichen Hinweis, dass es sich hierbei um medizinische Unterlagen handelt, hätte zu einer richtigen Zustellung geführt. Dem Arzt muss hier zu Recht vorgehalten werden, nicht sorgfältig und der Sensitivität der Daten entsprechend gehandelt zu haben.

3.8.4.2.3
Nutzung der Daten durch den Fachdienst Verkehr

Schließlich stellte sich aber die Frage, ob der Fachdienst Verkehr die Unterlagen, die nicht für ihn bestimmt waren, dennoch verwenden durfte. Hier berief sich die zuständige Führerscheinstelle des Wetteraukreises (als Teil des Fachdienstes Verkehr) auf § 11 Abs. 2 der Fahrerlaubnisverordnung. Für Inhaber einer Fahrerlaubnis gilt diese Vorschrift i. V. m. § 46 Abs. 3 auch für eine Entziehung, Beschränkung oder Auflagen einer Fahrerlaubnis. Werden danach Tatsachen bekannt, die Bedenken gegen die körperliche oder geistige Eignung begründen, kann die Behörde die Beibringung eines ärztlichen Gutachtens durch den Bewerber anordnen.

§ 46 Abs. 3 FeV

Werden Tatsachen bekannt, die Bedenken begründen, dass der Inhaber einer Fahrerlaubnis zum Führen eines Kraftfahrzeugs ungeeignet oder bedingt geeignet ist, finden die §§ 11 bis 14 entsprechend Anwendung.

§ 11 Abs. 2 FeV

Werden Tatsachen bekannt, die Bedenken gegen die körperliche oder geistige Eignung des Fahrerlaubnisbewerbers begründen, kann die Fahrerlaubnisbehörde zur Vorbereitung von Entscheidungen über die Erteilung oder Verlängerung der Fahrerlaubnis oder über die Anordnung von Beschränkungen oder Auflagen die Beibringung eines ärztlichen Gutachtens durch den Bewerber anordnen.

Unbeachtet lässt diese Regelung, auf welche Weise die Tatsachen bekannt wurden. Unerheblich ist deshalb auch, ob in diesem Fall die Daten nur zufällig oder unbeabsichtigt die hierfür zuständige Behörde erreichen. Das schließt freilich nicht aus, dass die Führerscheinstelle der Verwendung der Daten eine pflichtgemäße Ermessensausübung voranzustellen hat. Die Informationen zu dem Gesundheitszustand des Betroffenen waren allerdings so aktuell und zudem gravierend, dass man der Führerscheinstelle eine unangemessene Vorgehensweise nicht unterstellen konnte. Die Prüfung der Eignung erfolgt, um sicherzustellen, dass andere Verkehrsteilnehmer nicht gefährdet werden (vgl. z. B. § 2 FEV). Die Verwendung der Daten war in Abwägung gegen das zu schützende Rechtsgut der Unversehrtheit der anderen Verkehrsteilnehmer zulässig.

3.9 Sozialwesen

3.9.1
Zusammenarbeit von SGB II-Stellen („Hartz IV“) mit Jugendämtern

Bei der Kooperation von Trägern der Grundsicherung für Arbeitsuchende und Trägern der öffentlichen Jugendhilfe sind unterschiedliche sozialdatenschutzrechtliche Regelungen maßgebend. Dies steht aber einer sinnvollen Zusammenarbeit dieser Stellen nicht im Wege.

3.9.1.1
Der Anlass

Der Arbeitskreis Hessischer Optionskommunen hat mich um Beratung gebeten, welche datenschutzrechtlichen Rahmenbedingungen für eine kontinuierliche Zusammenarbeit mit den Jugendämtern gelten. Es geht bei diesem Projekt darum, Jugendliche in prekärer Situation durch gemeinsame Unterstützung zu fördern.

3.9.1.2
Sozialrechtliche Vorgaben

Die Zusammenarbeit von SGB II- und SGB VIII-Stellen ist gesetzlich ausdrücklich vorgesehen (§§ 18 SGB II, 13, 81 SGB VIII), und ganz dementsprechend hat die Bundesregierung zum Verhältnis dieser Verwaltungszweige Folgendes ausgeführt (BTDrucks. 17/2083, S. 5):

Sowohl das SGB VIII als auch das SGB II haben einen eigenständigen Leistungs- und Geltungsbereich mit den entsprechenden Zielsetzungen. Aus den unterschiedlichen Leistungssystemen folgen unterschiedliche Zuständigkeiten von Trägern der Grundsicherung für Arbeitsuchende und öffentlichen Jugendhilfeträgern. Die Grundsicherung für Arbeitsuchende ist in ihrer Zielsetzung klar auf eine Eingliederung in den Arbeitsmarkt und die damit verbundene Überwindung der Hilfebedürftigkeit gerichtet. Die Jugendhilfe spricht demgegenüber von einem Recht auf Förderung der Entwicklung eines Jugendlichen und seiner Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit. Im Einzelfall müssen deshalb Hilfen aus beiden Leistungssystemen parallel und in Ergänzung

zueinander erbracht werden. Daraus ergeben sich Schnittstellen, die es in der Praxis durch eine entsprechende Zusammenarbeit möglichst reibungslos zu bewältigen gilt. Der Gesetzgeber hat den Auftrag zur Zusammenarbeit der Träger der Grundsicherung für Arbeitsuchende und der Träger der Kinder- und Jugendhilfe in den jeweiligen Leistungsgesetzen formuliert (§§ 18 SGB II, 81 SGB VIII). Systembrüche kann die Bundesregierung insofern nicht erkennen.

Auch in der Presse ist diese Zusammenarbeit näher thematisiert worden, und dies mit dem knappen datenschutzrechtlichen Hinweis, dass der Austausch von Daten zwischen diesen Stellen „ein heikles Thema“ sei (so FAZ vom 3. September 2010 S. 41).

3.9.1.3 Datenschutzrechtliche Aspekte

Die Übermittlung von Sozialdaten seitens des Jobcenters an das Jugendamt ist im Kapitel 6. des SGB II (Datenerhebung, -verarbeitung und -nutzung, datenschutzrechtliche Verantwortung) nicht geregelt (§§ 50 ff. SGB II). Maßgebend ist vielmehr das im SGB X platzierte allgemeine Sozialdatenschutzrecht, und zwar die Übermittlungsvorschrift § 69 SGB X, die für die Datenübermittlung zwecks Aufgabenwahrnehmung nach dem SGB die zentrale Vorschrift ist.

§ 69 Abs. 1 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist

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

Im vorliegenden Kontext bedeutet dies konkret, dass Jobcenter Sozialdaten an Jugendämter übermitteln können, wenn es für die Aufgabenerfüllung des Jobcenters oder des Jugendamtes erforderlich ist. Für die Zusammenarbeit von Jobcentern und Jugendämtern ist diese Regelung geradezu idealtypisch, weil einzige Bedingung für die Datenübermittlung seitens der Jobcenter die Erforderlichkeit für die Aufgabenwahrnehmung nach dem SGB II oder dem SGB VIII ist.

Im Vergleich zu den Jobcentern sind die datenschutzrechtlichen Vorgaben für die Jugendämter restriktiver als § 69 Abs. 1 Nr. 1 SGB X. Denn für die Datenübermittlung seitens der Jugendämter an die Jobcenter reicht es beispielsweise nicht schon aus, dass die Datenübermittlung für die Aufgabenwahrnehmung des Jobcenters erforderlich ist. Das Jugendamt muss näm-

lich zusätzlich für sich die Frage klären, ob eine Datenübermittlung an das Jobcenter den Erfolg der eigenen Arbeit beeinträchtigen könnte (§ 64 Abs. 2 SGB VIII).

§ 64 Abs. 2 SGB VIII

Eine Übermittlung für die Erfüllung von Aufgaben nach § 69 des Zehnten Buches ist ... nur zulässig, wenn dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.

In Einzelfällen kann neben § 64 Abs. 2 SGB VIII auch § 65 SGB VIII eine weitere rechtliche Übermittlungssperre sein. Eine solche Konstellation liegt dann vor, wenn ein Betroffener Sozialdaten speziell einem Mitarbeiter des Jugendamtes anvertraut hat (näher zu dieser Situation etwa Rombach in Hauck, SGB VIII, § 65 Rn. 3). In diesem Fall liegt von wenigen Ausnahmen abgesehen ein behördeninternes Weitergabeverbot vor, was erst recht einer Übermittlung an eine externe Stelle (hier: Jobcenter) entgegensteht.

§ 65 Abs. 1 und 2 SGB VIII

(1) Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesen nur weitergegeben werden ...

(2) § 35 Abs. 3 des Ersten Buches gilt auch, soweit ein behördeninternes Weitergabeverbot nach Abs. 1 besteht.

In § 35 Abs. 3 des Ersten Buches wird das Verbot der Weitergabe von Sozialdaten präzisiert.

§ 35 Abs. 3 SGB I

Soweit eine Übermittlung nicht zulässig ist, besteht keine Auskunftspflicht, keine Zeugnispflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken, nicht automatisierten Dateien und automatisiert erhobenen, verarbeiteten oder genutzten Sozialdaten.

Die angeführte Rechtslage habe ich auf der vom Arbeitskreis Hessischer Optionskommunen initiierten Veranstaltung, die die Zusammenarbeit von Jobcentern und Jugendämtern als Schwerpunktthema hatte, vorgetragen und in ihren Details näher erläutert.

3.9.2
Sozialdatenschutz und Kommunalaufsicht

Die staatliche Kommunalaufsicht ist befugt, von einem kommunalen Jugendamt die Übermittlung von Sozialdaten zu verlangen. Der kinder- und jugendhilferechtliche Sozialdatenschutz steht einer Übermittlung nur ausnahmsweise entgegen.

3.9.2.1
Der Anlass

Das Regierungspräsidium Darmstadt legte mir die Frage vor, ob der Sozialdatenschutz der Ausübung der kommunalrechtlichen Rechtsaufsicht über einen Landkreis entgegenstehen könne. Konkret ging es darum, dass ein Kreisjugendamt sich weigerte, dem Regierungspräsidium Darmstadt Auskünfte zu geben, und diese Weigerung mit dem Sozialdatenschutz begründete.

3.9.2.2
Datenschutzrechtliche Bewertung

Die Kommunalaufsicht ist in den §§ 135 ff. HGO geregelt.

§ 135 HGO

Die Aufsicht des Staates über die Gemeinden soll sicherstellen, dass die Gemeinden im Einklang mit den Gesetzen verwaltet und dass die im Rahmen der Gesetze erteilten Weisungen (§ 4) befolgt werden. Die Aufsicht soll so gehandhabt werden, dass die Entschlusskraft und die Verantwortungsfreudigkeit der Gemeinden nicht beeinträchtigt werden.

Die Aufsicht kann auch in der Weise ausgeübt werden, dass von der Kommune Informationen in der jeweiligen Angelegenheit angefordert werden (§ 137 HGO).

§ 137 HGO

Die Aufsichtsbehörde kann sich jederzeit über die Angelegenheiten der Gemeinden unterrichten; sie kann an Ort und Stelle prüfen und besichtigen, Berichte anfordern sowie Akten und sonstige Unterlagen einsehen.

Gemäß § 54 Hessischer Landkreisordnung (HKO) gelten die in den §§ 135 ff. HGO getroffenen Regelungen für die Aufsicht über die Landkreise entsprechend.

Der Kommunalaufsicht steht das kinder- und jugendhilferechtliche Sozialdatendatenschutzrecht (§§ 61 ff. SGB VIII) grundsätzlich nicht entgegen. Denn im SGB VIII wird ausdrücklich auf die Anwendbarkeit des insbesondere im SGB X geregelten Sozialdatenschutzes verwiesen (§ 61 Abs. 1 SGB VIII), und nicht nur im allgemeinen Datenschutzrecht, sondern auch im Sozialdatenschutzrecht ist die Datenverwendung zu Aufsichts- und Kontrollzwecken privilegiert. Im Sozialdatenschutzrecht ist das in den §§ 67c Abs. 3, 69 Abs. 5 SGB X ausdrücklich so geregelt.

§ 67c Abs. 3 SGB X

Eine Speicherung, Veränderung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie für die Wahrnehmung von Aufsichts-, Kontrollbefugnissen ... erforderlich ist.

§ 69 Abs. 5 SGB X

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

Diese Regelungen haben zur Konsequenz, dass ein Regierungspräsidium als Kommunalaufsichtsbehörde personenbezogene Informationen vom Kreisjugendamt im Regelfall anfordern kann.

Allerdings sieht das spezielle kinder- und jugendhilferechtliche Datenschutzrecht Ausnahmen vor.

Beispielsweise wäre eine Übermittlung von Sozialdaten seitens des Jugendamtes an das Regierungspräsidium zu Aufsichts- und Kontrollzwecken unzulässig, wenn dadurch der Erfolg der Aufgabenwahrnehmung des Jugendamtes in einer bestimmten Angelegenheit gefährdet würde, (§§ 64 Abs. 2 SGB VIII, 69 Abs. 5 SGB X). Es geht dann aber letztlich nicht um Datenschutz, sondern um Schutz von bestimmten Betreuungsverhältnissen.

§ 64 Abs. 2 SGB VIII

Eine Übermittlung für die Erfüllung von Aufgaben nach 69 des Zehnten Buches ist ... nur zulässig, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.

Neben dem § 64 Abs. 2 SGB VIII kann auch § 65 SGB VIII einer Übermittlung entgegenstehen, wenn nämlich speziell einem Mitarbeiter des Jugendamtes in der persönlichen und erzieherischen Hilfe Sozialdaten anvertraut worden sind (näher zu dieser Konstellation bspw. Rombach in Hauck, SGB VIII § 65 Rdnr. 3). In diesem Fall besteht sogar ein behördeninternes Weiter-

gabeverbot, sodass eine Übermittlung an eine andere, externe Behörde erst recht nicht in Betracht kommt.

§ 65 SGB VIII

(1) Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden...

(2) § 35 Abs. 3 des Ersten Buches gilt auch, soweit ein behördeninternes Weitergabeverbot nach Abs. 1 besteht.

Ich habe das Regierungspräsidium Darmstadt über diese Rechtslage betreffend das Verhältnis von Kommunalaufsicht und Sozialdatenschutz im Kinder- und Jugendhilfebereich informiert.

3.9.3
Recherche in sozialen Netzwerken durch SGB II-Stellen (Jobcenter)

Eine Datenerhebung der Sozialverwaltung in sozialen Netzwerken ist ohne konkreten Anlass in einem begründeten Einzelfall unzulässig. Diese Möglichkeit der Datenerhebung steht als generelles Instrument nicht zur Verfügung.

Ein behördlicher Datenschutzbeauftragter eines Landkreises und einer SGB II-Stelle stellte mir die Frage, inwieweit Sozialleistungsträger Recherchen in sozialen Netzwerken wie z. B. Facebook® oder wer-kennt-wen durchführen und hierdurch gewonnene Informationen (z. B. sog. Statusmeldungen wie „Ich war im Urlaub“, „Ich habe einen neuen Job“) verwerten dürfen, um möglichen Leistungsmissbrauch aufzudecken.

Ich habe den Landkreis darauf hingewiesen, dass ich die Erhebung und Verwendung von Daten aus sozialen Netzwerken wie Facebook®, wer-kennt-wen o. Ä. durch Sozialleistungsträger – von Ausnahmen abgesehen – für rechtswidrig halte.

Auch im Sozialrecht und hier bei den gesetzlichen Bestimmungen zur Datenerhebung, -verarbeitung und -nutzung, §§ 67a ff. SGB X, gilt grundsätzlich das Prinzip der Erhebung von Sozialdaten direkt beim Betroffenen (§ 67a Abs. 2 Satz 1 SGB X; Grundsatz der Direkterhebung). Das Sozialgeheimnis gewährt dem Betroffenen den Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (§ 35 Abs. 1 Satz 1 SGB I). § 35 Abs. 2 SGB I verweist sodann für die zulässige Erhebung, Verarbeitung und Nutzung von Sozialdaten auf die Voraussetzungen des Zweiten Kapitels SGB X.

Die Erhebung von Daten über Betroffene/Leistungsempfänger in den o. g. sozialen Netzwerken lässt sich im Rahmen von § 67a SGB X nicht rechtfertigen.

Das mögliche Gegenargument, nämlich die Geltung des Untersuchungsgrundsatzes gemäß § 20 SGB X, wonach die Behörde den Sachverhalt von Amts wegen ermittelt und dabei Art und Umfang der Ermittlungen bestimmt, kommt nicht zum Tragen. Denn § 37 Satz 3 SGB I bestimmt, dass das Zweite Kapitel SGB X dessen Erstem Kapitel vorgeht, soweit sich die Ermittlung des Sachverhalts auf Sozialdaten erstreckt.

Darüber hinaus ist nicht auszuschließen, dass bei einer Recherche, beabsichtigt oder unbeabsichtigt, möglicherweise eine Vielzahl von Daten über die Betroffenen erhoben wird, die für die sozialgesetzliche Aufgabenerfüllung der Behörde nicht erforderlich sind. Zu diesem Ergebnis führt auch die notwendige Interessenabwägung im Vorfeld einer solchen Maßnahme/Recherche, bei der es um eine Abwägung der Erforderlichkeit hinsichtlich des zu erfüllenden Zwecks und der schutzwürdigen Interessen der Betroffenen ginge.

Nur in einem besonderen Ausnahme-, einem konkreten Einzelfall, bei dem gravierende tatsächliche Anhaltspunkte (keine reinen Verdachtsmomente) für einen Leistungsmissbrauch o. Ä. vorliegen, die auch nicht unmittelbar mit dem Betroffenen selbst und direkt geklärt werden können, liegt eine Ausnahme vom o. g. Grundsatz vor.

Im Übrigen habe ich, da die Fallkonstellation hinsichtlich der Datenerhebung vergleichbar ist, auf den Entwurf der Bundesregierung zur Regelung des Beschäftigungsdatenschutzes hingewiesen, speziell auf § 32 Abs. 6 BDSG-E (BTDrucks. 17/4230, Seite 6).

§ 32 Abs. 6 BDSG-E

Beschäftigtendaten sind unmittelbar beim Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind. …

Im Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Kabinettbeschluss vom 25. August 2010, heißt es zu § 32 Abs. 6 BDSG-E:

Der Arbeitgeber darf sich grundsätzlich über einen Bewerber aus allen allgemein zugänglichen Quellen (z. B. Zeitung oder Internet) informieren. Eine Einschränkung der Informationsmöglichkeiten des Arbeitgebers sieht der Gesetzentwurf hinsichtlich sozialer Netzwerke im Internet vor. Soweit soziale Netzwerke der Kommunikation dienen (z. B. Facebook, schülerVZ, studiVZ, StayFriends), darf sich der Arbeitgeber daraus nicht über den Bewerber informieren. Nutzen darf der Arbeitgeber jedoch soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind (z. B. Xing, LinkedIn). Damit soll der Ausforschung privater, nicht zur Veröffentlichung bestimmter Daten entgegengewirkt werden.

Die Begründung der Bundesregierung für ihren Gesetzentwurf zu § 32 Abs. 6 BDSG präzisiert diese Ausführung (ebenda Seite 17):

… Allgemein zugänglich sind Daten z. B. dann, wenn sie der Presse oder dem Rundfunk zu entnehmen sind. Auch im Internet bei bestimmungsgemäßer Nutzung für jeden abrufbare Daten sind grundsätzlich allgemein zugänglich, insbesondere, wenn die Daten über eine allgemeine Suchmaschine auffindbar sind. Sind die eingestellten Daten dagegen nur einem beschränkten Personenkreis zugänglich, z. B. ausgewählten Freunden, liegt eine allgemeine Zugänglichkeit nicht vor. Die Erhebung allgemein zugänglicher Daten ist nicht zulässig, wenn das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung gegenüber dem berechtigten Interesse des Arbeitgebers überwiegt. Einen solchen Fall regelt ausdrücklich Satz 2 letzter Halbsatz im Hinblick auf soziale Netzwerke im Internet, die der elektronischen Kommunikation dienen. Die dort eingestellten Daten dürfen vom Arbeitgeber grundsätzlich nicht erhoben werden; eine Ausnahme hiervon gilt nur für soziale Netzwerke im Internet, die gerade zur eigenen Präsentation gegenüber potentiellen Arbeitgebern genutzt werden. Überwiegende schutzwürdige Interessen des Beschäftigten können sich im Übrigen daraus ergeben, wie alt die Veröffentlichung der Daten im Internet ist, in welchem Kontext sie erfolgt und ob der Beschäftigte nach den erkennbaren Umständen noch die Herrschaft über die Veröffentlichung hat. …

Dem behördlichen Datenschutzbeauftragten des Landkreises habe ich meine Rechtsauffassung mitgeteilt. Das Hessische Sozialministerium, welches durch den Datenschutzbeauftragten des Landkreises ebenfalls um Stellungnahme zu seiner Fragestellung gebeten wurde, hat sich meiner Rechtsauffassung angeschlossen.

3.10 Personalwesen

3.10.1
Observierung und Verwertungsverbot

Für eine unverhältnismäßige Überwachung eines Beschäftigten gibt es keine Rechtsgrundlage. Die Erkenntnisse aus einer solchen Überwachung können einem Verwertungsverbot unterliegen.

3.10.1.1
Der Konflikt

Ein Beschäftigter in einer nordhessischen Kreisverwaltung beschwerte sich bei mir darüber, dass er von einem Mitglied des Kreisausschusses (Ehrenamtlicher Beigeordneter) bespitzelt worden sei. Konkret ging es darum, dass der Beigeordnete und der Beschäftigte Grundstücksnachbarn sind und der Beigeordnete über einen Zeitraum von zumindest mehreren Monaten aktenkundig vermerkte, zu welchen Zeiten der Beschäftigte auf seinem Grundstück anwesend war. Dies führte zu einem disziplinarrechtlichen Verweis gegen den Beschäftigten wegen angeblicher Arbeitszeitverstöße.

3.10.1.2
Das verwaltungsgerichtliche Verfahren

Ich habe den Kreisausschuss seinerzeit darauf hingewiesen, dass die Observierung seitens des Beigeordneten eine unverhältnismäßige und damit rechtswidrige Überwachung des Beschäftigten gewesen und es deshalb eine naheliegende Folgerung sei, von einem Verwertungsverbot der Bespitzelungsergebnisse auszugehen. Vor diesem Hintergrund habe ich den Kreisausschuss aufgefordert, das Disziplinarverfahren einzustellen. Dieser Aufforderung kam der Kreisausschuss allerdings nicht nach, sondern wies den Widerspruch des Beschäftigten gegen den Verweis zurück. Daraufhin reichte der Beschäftigte Klage beim Verwaltungsgericht in Kassel ein.

Mit Rücksicht auf diesen Verwaltungsgerichtsprozess habe ich in meinem letzten Tätigkeitsbericht davon abgesehen, die Angelegenheit zu thematisieren. Zum Zeitpunkt der Vorstellung meines letzten Tätigkeitsberichtes war die Observierung gleichwohl über die Presse an die Öffentlichkeit gelangt. Vor diesem Hintergrund habe ich auf der Pressekonferenz die unverhältnismäßige Überwachung zwar gerügt, aber auch auf das laufende verwaltungsgerichtliche Verfahren verwiesen.

Mittlerweile hat sich das Verwaltungsgericht Kassel meiner Rechtsauffassung betreffend das Verwertungsverbot angeschlossen (Az.: 28 K 1788/10.KS.D). Sein dementsprechender Hinweis an den beklagten Landkreis hat dazu geführt, dass der Kreis Verweis und Widerspruchsbescheid aufgehoben hat.

3.10.2
Beihilfebearbeitung im Auftrag von Kreisen, Städten und Gemeinden durch eine Versorgungskasse

Sinn und Zweck der Vorschrift zu Beihilfeunterlagen ist der Schutz des Persönlichkeitsrechts der Beamtinnen und Beamten. Durch die besonderen Regelungen zur Aktenführung der Beihilfeunterlagen werden nachteilige Folgen für diese im Verlaufe des Beamtenverhältnisses vermieden. Vor diesem Hintergrund sollen die Beihilfeakten in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden.

3.10.2.1
Der Sachverhalt

In einer südhessischen Kommune habe ich u. a. den dortigen Fachbereich Personalservice geprüft. Dabei wurde ich darauf aufmerksam, dass es dort trotz Übertragung der Beihilfebearbeitung an eine Versorgungskasse umfangreiche Vorgänge zu Beihilfeangelegenheiten gab.

So wurde über den Versand und den Eingang von Beihilfeanträgen bzw. -bescheiden in der Personalabteilung Buch geführt. Hier war u. a. vermerkt: Eingang eines Beihilfeantrages in der Personalabteilung, Weitergabe des Beihilfeantrages an die Versorgungskasse, Eingang des Beihilfebescheides von der Versorgungskasse, interne Weiterleitung an den Antragsteller. Die Personalabteilung erhielt von jedem Beihilfebescheid der Versorgungskasse einen Abdruck. Dieser Abdruck entsprach demjenigen, den der Antragsteller persönlich auch bekam, und enthielt Angaben u. a. dezidiert zu jedem einzelnen Beleg (Rechnung, Rezept, etc.), den Namen des behandelnden oder verordnenden Arztes und die Höhe der jeweiligen Erstattung. Nach Ansicht der Personalleitung war dies in dieser Form auch erforderlich, da die Personalleitung für die Beihilfeabrechnung verantwortlich sei und „sachlich/rechnerisch richtig“ zu bestätigen und vermerken habe.

3.10.2.2
Datenschutzrechtliche Bewertung

§ 92 HBG regelt die Fürsorgepflicht des Dienstherrn. § 92 Abs. 2 HBG bestimmt, dass den Beamten und den Empfängern von Versorgungsbezügen in Krankheits-, Geburts- und Todesfällen sowie zu Aufwendungen für Maßnahmen zur Gesundheitsvorsorge, zur Früherkennung von Krankheiten, für nicht rechtswidrige Schwangerschaftsabbrüche und nicht rechtswidrige Sterilisationen Beihilfen gewährt werden. § 92 Abs. 3 betrifft die Übertragung der Beihilfeaufgaben.

§ 92 Abs. 3 HBG

Zur Erfüllung seiner Verpflichtungen nach Abs. 2 kann sich der Dienstherr geeigneter Stellen auch außerhalb des öffentlichen Dienstes bedienen und diesen die zur Beihilfebearbeitung erforderlichen Daten übermitteln. Die beauftragte Stelle darf die Daten, die ihr im Rahmen der Beihilfebearbeitung bekannt werden, nur für diesen Zweck verarbeiten. § 107a und § 107g Abs. 2 sowie § 4 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999 (GVBl. I S. 98) gelten entsprechend.

Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren (§ 107a Abs. 1 Satz 1 und 2 HBG). Bei automatisierter Beihilfebearbeitung (§ 107g Abs. 2 HBG) ist ausnahmsweise die Zusammenfassung der Beihilfebescheide in Sachakten zulässig, sofern der Datenschutz gesichert und gewährleistet ist, dass die Beihilfe-Teilakte jederzeit wieder zusammengeführt werden kann (§ 107a Abs. 1 Satz 4 HBG). Personalaktendaten im Sinne des § 107a HBG dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden (§ 107g Abs. 2 HBG).

§ 107a Abs. 1 HBG

Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Bei automatisierter Beihilfebearbeitung (§ 107g Abs. 2) ist ausnahmsweise die Zusammenfassung der Beihilfebescheide in Sachakten zulässig, sofern der Datenschutz gesichert und gewährleistet ist, dass die Beihilfe-Teilakte jederzeit wieder zusammengeführt werden kann.

Beihilfeakten enthalten sehr sensible Daten von Bediensteten, ggf. auch von ihren Familienangehörigen. Jeder, der im Einzelfall berechtigt auf Personalhaupt- oder Teilakten zugreifen kann, darf nicht mit Beihilfeakten bzw. -vorgängen befasst werden. Gemäß § 107a Abs. 1 Satz 3 HBG **soll** daher die Beihilfebearbeitung in einer von der übrigen Personalverwaltung getrennten Organisationseinheit vorgenommen werden. Zugang **sollen** nur Beteiligte dieser Organisationseinheit haben. Die Sollvorschrift in § 107a Abs. 1 Satz 3 HBG berücksichtigt die Schwierigkeiten kleinerer Behörden. Dort ist es wegen der geringen Zahl der Bediensteten und der Sicherstellung der Vertretung oft nicht möglich, eine getrennte Bearbeitung von Personalangelegenheiten einerseits und Beihilfeangelegenheiten andererseits durchzuführen. Soweit jedoch in einer Behörde die Trennung der Bearbeitung möglich ist – und dies ist der Regelfall –, muss die Beihilfebearbeitung von der übrigen Personalverwaltung getrennt werden.

Auch eine „Vorprüfung“ von Beihilfeanträgen durch die Personalabteilung einer Dienststelle widerspricht dem gesetzlich vorgesehenen Trennungsgebot von Personalabteilung und Beihilfebearbeitung.

Anlässlich dieses Falles und der Organisation der Abläufe sowohl bei der Kommune als auch bei der beauftragten Versorgungskasse habe ich mit dem Hessischen Ministerium des Innern und für Sport Kontakt aufgenommen. Dies mit der Bitte um eine Stellungnahme bezüglich der Auslegung der auf die Verwaltungsorganisation bezogenen beihilferechtlichen Vorschriften der §§ 92 und 107a HBG. Das Ministerium hat sich meiner Rechtsauffassung angeschlossen. Es betont ebenfalls, dass ein Dienstherr mit einer entsprechenden Organisationsstruktur für die Einhaltung dieser Vorgaben Sorge tragen muss und die Kommune sicherzustellen hat, dass die Übersendung von Unterlagen durch die private Stelle (Versorgungskasse) an ihre Organisation zu einer von der übrigen Personalverwaltung abgetrennten Einheit erfolgt.

Es hat einer längeren Intervention bedurft, um dem Personalaktenrecht betreffend Beihilfedaten bei der südhessischen Kommune zum Durchbruch zu verhelfen. Die Bearbeitung der Beihilfeangelegenheiten erfolgt dort nun in einer von der Personalverwaltung abgetrennten Organisationseinheit. Der Versorgungskasse wurde außer durch mich zusätzlich durch das Hessische Ministerium des Innern und für Sport mitgeteilt, dass dem bei der Adressierung der Beihilfeunterlagen Rechnung getragen wird. Die Weitergabe von Beihilfeunterlagen an die Kommune kann unter diesen Voraussetzungen im Hinblick auf die ihr nach den §§ 107a Abs. 1 bis 3, 107f Abs. 2 Satz 1 HBG obliegenden Pflichten dann gerechtfertigt werden.

3.10.3
Löschung von Daten im SAP R/3 HR-System

Die Löschung der urlaubs- und krankheitsbedingten Abwesenheiten nach Ablauf der Aufbewahrungsfristen ist in SAP R/3 HR jetzt möglich. Konzepte zur Umsetzung der weiteren gesetzlich vorgeschriebenen Löschungen werden noch erarbeitet.

Die Umsetzung der gesetzlich vorgeschriebenen Löschungen in SAP R/3 HR war bereits Gegenstand meines 36. Tätigkeitsberichts (Ziff. 5.10.3.2) und hat mich seither immer wieder beschäftigt (38. Tätigkeitsbericht, Ziff. 4.8.3; 39. Tätigkeitsbericht, Ziff. 4.1.5).

Der neu entwickelte Löschreport zum Löschen von krankheits- und urlaubsbedingten Abwesenheiten wurde nunmehr am 7. April 2011 produktiv

gesetzt. Mit diesem Report können die urlaubs- und krankheitsbedingten Daten bis einschließlich 31. Dezember 2006 gelöscht werden. Die Durchführung der Löschung der Daten mit diesem Löschlauf ist Voraussetzung für den Einsatz eines weiteren Löschreports, mit dem die Daten bis einschließlich 31. Dezember 2007 gelöscht werden können, deren Löschfrist auch im April 2011 bereits abgelaufen war.

Unter Hinweis auf die Tatsache, dass die Verantwortung für die Durchführung der Löschläufe bei den jeweils zuständigen personal führenden Stellen liegt, wurden die entsprechenden Informationen und technischen Hinweise den Anwendern per SAP-Mail bekannt gegeben.

Ich habe festgestellt, dass einige personal führende Stellen den 1. Löschlauf relativ zeitnah nach dem 7. April 2011 eingesetzt haben, so dass davon ausgegangen werden kann, dass auch die zu löschenden Daten bis einschließlich 31. Dezember 2007 zeitnah gelöscht wurden. Eine entsprechende Auswertung liegt mir zurzeit allerdings noch nicht vor.

Eine Auswertung der SAP-Datenbank hat ergeben, dass am 1. November 2011 noch insgesamt 7.559 Personaldatensätze gespeichert waren, bei denen die urlaubs- und krankheitsbedingten Daten aus der Zeit vor dem 31. Dezember 2006 noch nicht gelöscht wurden.

Es handelt sich um:

35	Datensätze im Bereich der Hessischen Landesvertretung in Berlin
360	Datensätze im Bereich des Innenministeriums
17	Datensätze im Bereich der Hessischen Polizeischule
224	Datensätze im Bereich der Polizei
2679	Datensätze im Bereich der Schulen
22	Datensätze im Bereich der Erwachsenenbildung
157	Datensätze im Bereich des Hessischen Kultusministeriums
350	Datensätze im Bereich der Staatlichen Schulämter
293	Datensätze im Bereich der Ämter für Lehrerfortbildung
18	Datensätze im Bereich des Hessischen Ministerium der Justiz
480	Datensätze im Bereich der ordentlichen Gerichtsbarkeit
180	Datensätze im Bereich der Staatsanwaltschaften
85	Datensätze im Bereich des Hessischen Finanzgerichts
464	Datensätze im Bereich des Justizvollzugs
349	Datensätze im Bereich der Verwaltungsgerichtsbarkeit
848	Datensätze im Bereich der Vorsorgekasse
18	Datensätze im Bereich der Steuerverwaltung

44 Datensätze im Bereich des Landesbetriebs Landwirtschaft Hessen
262 Datensätze im Bereich des Landesbetriebs Hessen-Forst
393 Datensätze im Bereich des Staatstheaters Kassel
313 Datensätze im Bereich des Staatstheaters Darmstadt

In dieser Auflistung sind nur die Buchungskreise enthalten, bei denen mehr als zehn Datensätze nicht gelöscht wurden. Bei allen betroffen Dienststellen können auch die zur Löschung anstehenden Daten des Jahres 2007 nicht gelöscht sein.

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

§ 107f Abs. 2 HBG

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

Die Angelegenheit wird zeitnah weiter geprüft. Gegebenenfalls werde ich die weitere Verarbeitung der Personaldatenverarbeitung mit dem SAP R/3 HR-System in der Hessischen Landesverwaltung gemäß § 27 HDSG beanstanden.

§ 27 HDSG

(1) Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. *bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,*
2. *bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.*

(2) Der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Mit der Beanstandung kann der Hessische Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Abs. 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Hessischen Datenschutzbeauftragten getroffen worden sind. Die in Abs. 1 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Hessischen Datenschutzbeauftragten zu.

Laut Mitteilung des Produktmanagements LRM HR soll bis zum 31. Dezember 2011 das Fachkonzept zum Löschen ganzer Datensätze im SAP R/3 HR-System erstellt werden. Auch in diesen Fällen sind die Fristen nach § 107f HBG bereits überschritten. Ich gehe davon aus, dass eine Umsetzung des zu erstellenden Löschreports bis Mitte 2012 möglich sein wird und werde die Realisierung der gesetzlich vorgeschriebenen Löschungen weiter datenschutzrechtlich begleiten.

3.10.4
Beteiligung meiner Behörde an verschiedenen Projekten im SAP R/3 HR-System

Auch in diesem Jahr hatte ich die Möglichkeit, bei der Entwicklung von Projekten der Neuen Verwaltungssteuerung und bei der Weiterentwicklung des SAP R/3 HR-Systems mitzuarbeiten. Somit konnten die datenschutzrechtlichen Belange schon in der konzeptionellen Phase berücksichtigt werden.

Das Projekt „Zentralisierung der Reisekosten-, Trennungsgeld- und Umzugskostenabrechnung bei der Hessischen Bezügestelle (HBS)“ wurde von mir während des ganzen Jahres eng begleitet und umfasste die Erstellung des Fachkonzepts und des erweiterten Fachkonzepts, in dem alle für die Zentralisierung dieser Aufgaben notwendigen fachlichen Anforderungen geprüft und einheitlich geregelt wurden. Bei den tiefgehenden Untersuchungen der fachlichen Anforderungen waren auch viele datenschutzrechtliche Fragen zu klären.

Ziel des Projekts ist es, die Bearbeitung der Reisekosten-, Trennungsgeld- und Umzugskostenabrechnung, die bisher im Land Hessen überwiegend dezentral stattfindet, bei der HBS zu zentralisieren und gleichzeitig eine automationsgestützte Bearbeitung der Abrechnungen auf Basis des SAP-Reisemanagement (SAP RM) zu realisieren und die sich durch den Wegfall der gesetzlichen Belegvorlagepflicht ergebenden Vereinfachungsmöglichkeiten zu nutzen. Weiterhin soll eine vollmaschinelle Bearbeitung unter Einbindung eines risikoorientierten Stichprobenverfahrens sowie einer Selbsterfassung durch die Antragsteller ermöglicht werden.

Die Projektleitung, in der ich beratend mitgearbeitet habe, tagte regelmäßig alle 14 Tage. In den Sitzungen wurden die Arbeitsergebnisse der einzelnen

Teilprojekte inhaltlich vorgestellt, offene Fragen geklärt und die notwendigen Entscheidungen getroffen.

Ebenso habe ich das im Jahr 2010 begonnene Projekt „Optimierung landesinterne Fortbildung“ bis zum März 2011 begleitet. Der Abschlussbericht und die dazugehörigen Unterlagen dieses Projekts wurden am 31. März 2011 an die Staatskanzlei weitergeleitet und waren am 11. April 2011 Thema auf der Tagesordnung des Kabinettsausschusses Verwaltungsmodernisierung.

Der Kabinettsausschuss hat ein Folgeprojekt beschlossen, das die Möglichkeit einer Informationsplattform für freie Tagungsstättenkapazität prüfen soll. Weiterhin soll geprüft werden, ob ein elektronischer Workflow für die technischen Prozesse der Fortbildungsorganisation durch den Einsatz von „SAP Enterprise Learning“ realisiert werden kann. Ebenso sollen die Voraussetzungen der fachlichen und rechtlichen Rahmenbedingungen und die Inhalte für ein landesweites Fortbildungscontrolling geprüft, sowie die Fortbildungsangebote der Ressorts in einem zentralen Fortbildungsportal transparent gemacht werden.

Mir wurde zugesagt, dass ich rechtzeitig auch weiterhin über die weitere Entwicklung informiert werde, um rechtzeitig die datenschutzrechtlichen Belange in diesem Projekt vertreten zu können.

Weiterhin werde ich im Lenkungsausschusses des Projekts „Optimierung der Personalverwaltung“, das von Staatssekretär Koch geleitet wird, über die Aktivitäten der Teilprojekte elektronische Personalakte, E-Recruting und Shared Service informiert.

Ich habe Gelegenheit, in allen Projekten die datenschutzrechtlichen Fragestellungen in die Diskussionen einzubringen und somit frühzeitig eine Klärung herbeizuführen.

Diese Form der rechtzeitigen Einbindung meiner Behörde hat sich aus meiner Sicht sehr bewährt. Erfahrungsgemäß sind Veränderung von festgelegten Verfahrensabläufen und bereits programmierten Verfahren aufgrund datenschutzrechtlicher Bedenken zu einem späteren Zeitpunkt nur sehr schwer und nur unter großem Aufwand zu realisieren.

4. Kommunale Selbstverwaltungskörperschaften

4.1
Veröffentlichung von Stellungnahmen zum Bebauungsplanverfahren im Internet

Einwendungen, die Bürger zu einem zur Stellungnahme ausliegenden Bebauungsplan abgeben, dürfen nicht personenbezogen im Internet veröffentlicht werden.

Zwei Bürger haben sich an meine Behörde gewandt und sich darüber beschwert, dass schriftliche Stellungnahmen von ihnen, die sie im Rahmen der Beteiligung gemäß § 3 Abs. 2 Baugesetzbuch zu einem Plankonzept für ein Wohngebiet abgegeben haben, als Teil einer Vorlage für eine Sitzung des Planungsausschusses der Stadt und für eine Sitzung der Stadtverordnetenversammlung im Internet veröffentlicht wurden.

Nach dem Baugesetzbuch (BauGB) sind die Bebauungspläne öffentlich auszulegen, dabei kann seit dem 1. Januar 2007 bei der Öffentlichkeits- und Behördenbeteiligung nach § 4a Abs. 4 BauGB ergänzend elektronische Informationstechnologie genutzt werden, um den Plan zu veröffentlichen.

§ 4a Abs. 4 BauGB eröffnet auch den Weg der Behördenbeteiligung und der Beteiligung der sonstigen Träger öffentlicher Belange in elektronischer Form. Über die Behandlung von Einwenderdaten natürlicher Personen enthält diese Vorschrift keine Regelung.

§ 4a Abs. 4 BauGB

Bei der Öffentlichkeits- und Behördenbeteiligung können ergänzend elektronische Informationstechnologien genutzt werden. Soweit die Gemeinde den Entwurf des Bauleitplans und die Begründung in das Internet einstellt, können die Stellungnahmen der Behörden und sonstigen Träger öffentlicher Belange durch Mitteilung von Ort und Dauer der öffentlichen Auslegung nach § 3 Abs. 2 und der Internetadresse eingeholt werden; die Mitteilung kann im Wege der elektronischen Kommunikation erfolgen, soweit der Empfänger hierfür einen Zugang eröffnet hat. Die Gemeinde hat bei Anwendung von Satz 2 Halbsatz 1 der Behörde oder dem sonstigen Träger öffentlicher Belange auf dessen Verlangen einen Entwurf des Bauleitplans und der Begründung zu übermitteln; § 4 Abs. 2 Satz 2 bleibt unberührt.

Es gelten somit für die Behandlung der Bürgereinwendungen die allgemeinen kommunalrechtlichen Grundsätze der HGO und des HDSG. Nach der HGO sind Sitzungen der Gemeindevertreter grundsätzlich öffentlich. Dies betrifft auch die Beratungen über Bauleitplanungen und die dagegen gerichteten Einwendungen. Dem liegt die Überlegung zugrunde, dass Planung ein diskursiver Prozess der wechselseitigen Beeinflussung ist. Pla-

nungsentscheidungen sollen in einem öffentlichen Dialog erfolgen. Dabei ist Öffentlichkeit als eine Präsenzöffentlichkeit vor Ort im Rahmen der Beratungen zu verstehen.

Die Veröffentlichung der personenbezogenen Daten aus dem Bebauungsplanverfahren im Internet geht aber weit über diesen Öffentlichkeitsgrundsatz hinaus, indem die Daten einem unbegrenzten Personenkreis zugänglich gemacht werden, der mit diesem Diskurs nichts zu tun hat. Bei sog. Jedermanneinwendungen fehlt das Interesse einer individuellen Zuordnung. Betroffeneneinwendungen sind nicht öffentlich. Ich habe deshalb die von der Stadt praktizierte Form der Veröffentlichung datenschutzrechtlich für unzulässig erklärt, da sie zu dem Entscheidungsprozess nicht erforderlich ist und schutzwürdige Belange einer Vielzahl von Personen beeinträchtigen kann.

Ich habe die Stadt aufgefordert, die Daten aus dem Internet zu entfernen und zukünftig die Stellungnahmen privater Personen nur noch in anonymisierter Form aufzunehmen. Die Stadt ist dieser Aufforderung gefolgt, entgegnete aber, dass das Internet zunehmend zur Plattform von Bürgerbeteiligung werde.

4.2
Unzulässiger Fingerprint beim Schwimmbadzugang

Fingerprintverfahren mögen als Zugangskontrolle zu Rechenzentren oder anderen besonders zu sichernden Anlagen das geeignete Kontrollsystem sein. Als Zugangskontrolle zu einem kommunalen Schwimmbad hingegen sind sie nicht zulässig.

Durch Bürgereingaben wurde ich darauf aufmerksam gemacht, dass eine hessische Kommune plante, den Zugang zu ihrem Schwimmbad neu zu regeln. Statt herkömmlicher Dauerkarten sollten Chipkarten ausgegeben werden, auf denen verschlüsselt ein Fingerprint gespeichert werden sollte. Damit erhoffte man sich, Personal einsparen zu können und Missbrauch von Dauerkarten abzustellen.

Gegen diese Planung richteten sich die Bürgereingaben. Ich habe daraufhin die Kommune angeschrieben und um Stellungnahme gebeten. Die Stadt bestätigte die Planungen und rechtfertigte sie mit dem Argument, dass die Fingerprints nicht in einer zentralen Datei, sondern lediglich auf der Chipkarte gespeichert würden, die in der Verfügung des jeweiligen Karteninhabers sei.

Daraufhin habe ich der Stadt dargelegt, dass ich die Erhebung dieser Daten aus datenschutzrechtlicher Sicht für unzulässig halte. Dieser Bewertung lagen folgende Erwägungen zu Grunde.

Die Erhebung derart sensibler Daten ohne eine bereichsspezifische Rechtsgrundlage halte ich für unzulässig. Ausweisdokumente wie der Reisepass müssen, Personalausweise dürfen Fingerabdrücke enthalten. Deren Erhebung ist jedoch normenklar im Pass- bzw. Personalausweisgesetz geregelt.

Die Zurverfügungstellung der Infrastruktureinrichtung „Schwimmbad“ ist Teil der durch die Stadt zu betreibenden Daseinsvorsorge und steht daher allen Bürgern offen. Im Rahmen dieser Aufgabenerfüllung ist die Stadt nicht berechtigt, Daten von Bürgern zu verarbeiten, deren Verarbeitung gesetzlich nur für eng begrenzte Bereiche vorgesehen ist.

Trotz dieser eindeutigen Stellungnahme hat die Stadt das Fingerprintsystem in Betrieb genommen. Ich sah mich deshalb gezwungen, das Vorgehen der Kommune nach § 27 Abs. 1 Satz 1 Nr. 2 HDSG zu beanstanden.

§ 27 Abs. 1 Satz 1 Nr. 2 HDSG

Stellt der Hessische Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

...

2. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 2 unterrichtet der Hessische Datenschutzbeauftragte gleichzeitig auch die zuständige Aufsichtsbehörde.

Gleichzeitig habe ich den zuständigen Landrat als Aufsichtbehörde über die Beanstandung in Kenntnis gesetzt.

Die Kommune führte in ihrer Stellungnahme gegenüber dem Landrat aus, dass sie aufgrund von Darlegungen des Städte- und Gemeindebundes das System dahingehend abgeändert habe, dass nun vor Ausgabe der Karte die Einwilligung in die Abgabe des Fingerprints von jedem Saisonkarteninhaber eingeholt werde. Wer keinen Fingerprint abgeben wolle, könne auch im Wege einer gleichwertigen Zugangsmöglichkeit das Schwimmbad betreten.

Ich habe gleichwohl an meiner Beanstandung festgehalten. Zunächst gab es keine gleichwertige Zugangsalternative. Besucher hätten unter Umständen längere Wartezeiten in Kauf nehmen müssen, um das Schwimmbad betreten zu können, da nicht beabsichtigt war, die Kassen dauerhaft zu besetzen. Vielmehr hätte u. U. Personal wie etwa der Schwimmmeister herbeigerufen werden müssen, um das Schwimmbad betreten zu können. Dies

kann nicht – von der Problematik des dann drohenden Aufsichtsdefizits abgesehen – als gleichwertig eingestuft werden.

Die Einführung eines Fingerprintsystems im Wege der Einwilligung halte ich zwar nicht ausnahmslos für unzulässig, sie unterliegt aber, wie dies im Übrigen auch der Städte- und Gemeindebund in seiner Stellungnahme zu dem System ausgeführt hat, der Prüfung, ob dieses Verfahren für den konkreten Zweck überhaupt verhältnismäßig ist. Diese Verhältnismäßigkeit war im konkreten Fall nicht gegeben. Wie das Bundesverfassungsgericht in ständiger Rechtsprechung (BVerfGE 65,1 ff; BVerfGE 93, 181 ff.) ausführt, ist ein Eingriff umso gravierender, je fragwürdiger der Nutzen der Datenverarbeitung ist.

Bei dem eingeführten Kassensystem handelte es sich um ein System, das

1. nicht fälschungssicher ist,
2. intensive Eingriffsqualität wegen mangelnder Alternative besitzt
3. und für weitere zukünftige Verfahren an Gewicht gewinnen kann; denn wenn schon für Leistungen einer Gemeinde im Rahmen der Daseinsvorsorge Fingerprints zum Einsatz kommen, dann ist zu befürchten, dass dies auch für die Leistungsverwaltung Schule machen könnte.

Zudem widerspricht die Nutzung eines derartigen Systems nach meiner Ansicht der Datenschutzkultur! Wie soll Kindern der Grundsatz der Datensparsamkeit nahegebracht werden, wenn sie schon beim Schwimmbadbesuch Fingerabdrücke abgeben sollen?

Die Kommunalaufsicht hat meine Bewertung geteilt und die Stadt angewiesen, das Kassensystem nicht weiter zu verwenden.

4.3
Keine Melderegisterauskünfte per Internet an Parteien und andere Träger von Wahlvorschlägen zu Wahlwerbezwecken

Für Gruppenauskünfte aus dem Melderegister an Parteien und andere Träger von Wahlvorschlägen über Internet gibt es keine gesetzliche Regelung und keine sichere Infrastruktur. Sie sind datenschutzrechtlich nicht zulässig.

Sechs Monate vor einer Wahl können Parteien und andere Träger von Wahlvorschlägen von der Meldebehörde Auskünfte von Wahlberechtigten erhalten. Bei diesen Melderegisterauskünften handelt es sich um sog. Gruppenauskünfte. Betroffen ist jeweils eine unbestimmte Vielzahl von Personen, deren Daten nach Lebensalter in Gruppen geordnet aus dem gesamten Meldedatenbestand ausgewertet werden. Übermittelt werden deren Vor-

und Nachname, Doktorgrad und Anschrift, § 35 Abs. 1 HMG, soweit sie einer Übermittlung nicht widersprochen haben.

§ 35 HMG

(1) Die Meldebehörde darf Parteien, anderen Trägern von Wahlvorschlägen und Wählergruppen im Zusammenhang mit Wahlen zum Deutschen Bundestag, zum Europäischen Parlament, mit Landtags- und Kommunalwahlen sowie mit Ausländerbeiratswahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über die in § 34 Abs. 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. ...

...

(5) Betroffene haben das Recht, der Weitergabe ihrer Daten nach Abs. 1 bis 4 zu widersprechen. Sie sind auf ihr Widerspruchsrecht bei der Anmeldung und spätestens acht Monate vor Wahlen oder Abstimmungen durch öffentliche Bekanntmachung hinzuweisen. ...

Bislang wurden diese Auskünfte von der Meldebehörde in ausgedruckten Listen bzw. auf anderen festen Medien, wie z. B. CDs, an die Empfänger übergeben.

Zunehmend bitten die Antragsteller die Meldebehörden diese – zum Teil sehr umfangreichen – Datenmengen „der Einfachheit halber“ per Internet zu übersenden. Das Melderecht sieht hierfür jedoch weder eine Rechtsgrundlage, noch einen datenschutzrechtlich geeigneten Übertragungsweg vor.

Für die Übermittlung von sog. einfachen Melderegisterauskünften nach § 34 Abs. 1 HMG, d. h. bei Anfragen nach einzelnen bereits durch den Namen bestimmten Personen gibt es zwar die Möglichkeit, das Internet über Online-Portale zu nutzen, § 34a HMG.

§ 34 Abs. 1 HMG

Personen, die nicht Betroffene sind, und anderen als den in § 31 Abs. 1 bezeichneten Stellen darf die Meldebehörde nur Auskunft über
1. Vor- und Familiennamen,
2. Doktorgrad und
3. Anschriften einzelner bestimmter Einwohnerinnen und Einwohner

übermitteln (einfache Melderegisterauskunft). Dies gilt auch, wenn jemand Auskunft über Daten einer Vielzahl namentlich bezeichneter Einwohnerinnen und Einwohner begehrt.

§ 34a HMG

(1) Einfache Melderegisterauskünfte nach § 34 Abs. 1 können auf automatisiert verarbeitbaren Datenträgern oder durch Datenübertragung erteilt werden, wenn
1. der Antrag in der amtlich vorgeschriebenen Form gestellt worden ist,

2. die Antragstellerin oder der Antragsteller die Betroffene oder den Betroffenen mit Vor- und Familiennamen sowie mindestens zwei weiteren der nach § 3 Abs. 1 gespeicherten Daten bezeichnet hat und
3. die Identität der oder des Betroffenen durch einen automatisierten Abgleich der im Antrag angegebenen mit den im Melderegister gespeicherten Daten der oder des Betroffenen eindeutig festgestellt worden ist.

...

(2) Einfache Melderegisterauskünfte können unter den Voraussetzungen des Abs. 1 Satz 1 auch mittels automatisierten Abrufs über das Internet erteilt werden. ...

(3) Der automatisierte Abruf über das Internet kann statt über den eigenen Zugang der Meldebehörde auch über elektronische Zugangsstellen (Portale) erfolgen. ...

Diese gesetzlichen Vorgaben gelten aber ausdrücklich nur für einfache Melderegisterauskünfte, also namentlich bestimmte Personen. Sie sind auf die Datenübermittlungen an Parteien und andere Träger von Wahlvorschlägen nicht übertragbar, da es sich bei der Gruppenauskunft um die Auswertung einer Vielzahl unbestimmter Betroffener handelt.

Die Übermittlung von Melderegisterauskünften außerhalb eines Online-Portals, z. B. über E-Mail, bietet wiederum weder ausreichende Sicherheitsmechanismen gegen Kenntnisnahme der Daten durch unberechtigte Dritte noch ermöglicht sie eine Identifikation und Authentisierung des Datenempfängers. Da zudem schon die Vielzahl der zu übermittelten Daten zu einem Datenmissbrauch durch „Abgreifen“ und Zweckentfremdung, z. B. Verkauf der Daten, verlocken kann, ist bewusst diese Form der Übermittlung im HMG nicht eröffnet.

Auf entsprechende Anfragen von Meldebehörden habe ich deshalb die Zulässigkeit der Übermittlung von Adressdaten wahlberechtigter Personen an Parteien oder andere Träger von Wahlvorschlägen über Internet abgelehnt.

4.4
Öffentliche Bekanntmachungen über melderechtliche Widerspruchsrechte

Eine ungeschickte Formulierung in einer öffentlichen Bekanntmachung über melderechtliche Widerspruchsrechte der Bürger gegen Melderegisterauskünfte erzeugte einen ungerechtfertigten Verdacht gegen das Meldeamt, dieses würde Daten zu Werbezwecken verkaufen.

Ein aufmerksamer Bürger hat sich an mich gewendet, weil er in einer amtlichen Bekanntmachung seiner Wohnsitzgemeinde gelesen hatte, dass das Einwohnermeldeamt neben den Melderegisterauskünften in besonderen Fällen nach § 35 HMG, der Internetauskunft nach § 34a HMG und der Aus-

kunft an öffentlich-rechtliche Religionsgemeinschaften nach § 32 Abs. 2 HMG auch privaten Dritten zum Zwecke der Direktwerbung Melderegisterauskünfte erteilt. Der Petent gewann durch diese Formulierung den Eindruck, dass die Kommune die Meldedaten an Firmen und Adresshändler verkauft. Tatsächlich waren aber nur die Formulierungen missverständlich.

Grundsätzlich sind die Kommunen nach § 35 Abs. 6 HMG verpflichtet, einmal jährlich die Einwohnerinnen und Einwohner auf Auskunftssperren nach dem Hessischen Meldegesetz hinzuweisen. Absicht der Kommune war es, mit der mit der mir übersandten amtlichen Bekanntmachung dieser gesetzlichen Verpflichtung nachzukommen.

§ 35 Abs. 6 HMG

Die Meldebehörden haben einmal jährlich und zusätzlich mindestens zwei Monate vor der Datenübermittlung an Adressbuchverlage die Einwohnerinnen und Einwohner über die Auskunftssperren nach diesem Gesetz zu unterrichten. Die Unterrichtung hat durch öffentliche Bekanntmachung in der durch die Hauptsatzung der Gemeinde vorgesehenen Form zu erfolgen. Dabei ist auf die Bedeutung, Arbeitsweise und Möglichkeiten von Adressbüchern auf elektronischen Datenträgern hinzuweisen. Die Datenübermittlung an Adressbuchverlage darf von der Übernahme der Kosten für die öffentliche Bekanntmachung abhängig gemacht werden.

In der Bekanntmachung wurden jedoch nicht die Rechte der Bürger dargestellt, sondern aufgezählt, welche Meldedatenübermittlungen das Einwohnermeldeamt vornimmt, wenn nicht ein Antrag auf Auskunftssperre gestellt oder entsprechende Widersprüche eingelegt wurden. Besonders irreführend war dies bei dem Hinweis auf „Auskunft an private Dritte zum Zwecke der Direktwerbung“. Bei dieser Widerspruchsmöglichkeit handelt es sich um einen Sonderfall, der nicht im Gesetzestext aufgeführt wird, sondern von der Rechtsprechung entwickelt wurde.

Grundsätzlich kann nach § 34 Abs. 1 HMG jede Privatperson von der Meldebehörde eine Auskunft über Namen, Doktorgrad und Anschriften einzelner, namentlich bestimmter Einwohnerinnen und Einwohner verlangen, ohne einen Grund für das Auskunftsbegehren zu nennen (einfache Melderegisterauskunft). Bevor das Meldeamt eine einfache Melderegisterauskunft erteilt, muss der Anfragende eine Verwaltungsgebühr bezahlen. Auf Klage eines Bürgers hat das Bundesverwaltungsgericht am 21. Juni 2006 (Az. 6 C 5/05) entschieden, dass Betroffene von der Meldebehörde verlangen können, die einfache Melderegisterauskunft nicht zu erteilen, wenn diese erkennbar für Zwecke der Direktwerbung begehrt wird.

Mit ihrem Hinweis wollte die Kommune auf diese zusätzliche Möglichkeit aufmerksam machen. Durch die gewählte Formulierung entstand bei dem

Petenten jedoch der Eindruck, dass Meldedaten von der Kommune für Direktmarketingzwecke „verkauft“ werden. Tatsächlich kommt in diesen Fällen die Kommune jedoch nur ihrer Verpflichtung nach Auskunft gegen Zahlung einer Verwaltungsgebühr nach.

Ich habe den Bürger über die Rechtslage informiert und die Kommune veranlasst, den Bekanntmachungstext so zu formulieren, dass der Bezug auf das Urteil des Bundesverwaltungsgerichts deutlich wird.

Ergänzend ist darauf hinzuweisen, dass diese Widerspruchsmöglichkeit nach dem Urteil des Bundesverwaltungsgerichts in der Praxis meist ins Leere laufen wird, da für die Anfrage nach einer einfachen Melderegisterauskunft grundsätzlich keine Begründung abgegeben werden muss. Die Meldeämter können im Regelfall also gar nicht erkennen, ob sich hinter einer Anfrage eine Absicht auf Nutzung für eine Direktwerbung verbirgt.

4.5
Trennung von IT-Netzen der Kommunen und kommunaler Gesellschaften

Bei einer Prüfung musste ich feststellen, dass eine Gesellschaft in kommunaler Hand auf Daten der Kommune zugreifen konnte, weil die Sicherheitsmaßnahmen unzureichend waren. Es fehlten auch die nötigen Verträge.

Wie in den letzten Jahren auch habe ich dieses Jahr die IT-Infrastruktur einiger Kommunalverwaltung geprüft. Neben den schon in den Vorjahren geschilderten Problemen (vgl. 36. Tätigkeitsbericht, Ziff. 6.1; 37. Tätigkeitsbericht, Ziff. 5.1) ergab sich ein weiterer Sachverhalt, der in vielen Kommunen relevant sein kann, da viele Kommunen ursprünglich städtische Abteilungen in kommunale Gesellschaften umwandeln.

Bei der Prüfung stellte sich heraus, dass unzulässige Datenzugriffe aus den Ämtern auf Sitzungsprotokolle von Magistratssitzungen möglich waren. Bei der Abklärung des Sachverhaltes gingen meine Mitarbeiter auch in die Räume einer eigenständigen städtischen Gesellschaft, die von der IT-Abteilung der Stadt mit betreut wurde. Von einem der dort vorhandenen Arbeitsplätze war mit einer Benutzerkennung der Gesellschaft ein Zugriff auf Daten der Stadt möglich. Dies betraf auch Daten von Bürgern wie den Ausdruck von Bescheiden.

Es zeigte sich, dass die Trennung der Datenbestände unzureichend war. Bis vor wenigen Jahren war die Gesellschaft noch ein städtisches Amt gewesen und man hatte sich entschieden, dessen Aufgaben in Form einer GmbH auszugliedern. Um den Aufwand möglichst gering zu halten, wurden die Strukturen möglichst wenig geändert, zu wenig wie sich gezeigt hat. Die

GmbH wurde von der netzseitigen Infrastruktur her fast wie ein städtisches Amt behandelt.

Erschwerend kam hinzu, dass es keine vertraglichen Regelungen gab, nach denen die IT-Abteilung der Stadt für die GmbH tätig wird.

Ich habe daher gefordert, technisch eine Trennung der Datenbestände und eine möglichst weit gehende Trennung der Netze vorzunehmen. Außerdem mussten Verträge zur Auftragsdatenverarbeitung nach § 4 HDSG geschlossen werden.

4.6
Serverdiebstahl beim Landratsamt Bad Hersfeld

Bei einem Einbruch kamen Anfang des Jahres Server mit samt den gespeicherten Daten abhanden. Es wurden erhebliche Anstrengungen unternommen, damals vorhandene Mängel zu beseitigen.

Anfang des Jahres wurde an einem Wochenende im Landratsamt Hersfeld-Rothenburg eingebrochen. Dabei wurden aus einem Serverraum die Server, sog. Blades, gestohlen. Teile von Datenbeständen waren auf diesen Rechnern gespeichert, sodass sie Unbefugten in die Hände gefallen sind.

Unmittelbar nachdem der Diebstahl bemerkt wurde, hat sich die Behörde mit mir in Verbindung gesetzt und mich über Abläufe und Reaktionen informiert. Von den in der Rückschau wichtigen räumlichen und anderen Sicherungsmaßnahmen möchte ich nur auf solche eingehen, die für andere Stellen bedeutsam sein können.

Gefährdungslage

Es gibt einen Markt für gestohlene Server. Server sind auf dem Schwarzmarkt viel wertvoller als PCs, sodass die Täter auch einen höheren Aufwand treiben und ein höheres Risiko eingehen, um Server zu stehlen. Diese Tatsache ist in vielen Sicherheitskonzepten noch nicht ausreichend berücksichtigt. So wird der Diebstahl von Arbeitsplatzrechnern als Gefährdung immer berücksichtigt und in vielen Fällen sehen die Konzepte vor, dass Daten nur noch auf den Servern gespeichert werden.

Diesem Schritt muss dann aber auch die ausreichende Sicherung der Server folgen.

Maßnahmen

– Es muss ein Konzept für die räumlichen Datensicherungsmaßnahmen geben, in das beispielsweise die Hinweise der kriminalpolizeilichen Beratungsstelle eingegangen sind.

– Die Eingänge (Türen, aber auch die Fenster) müssen so gesichert sein, dass nach der Auslösung eines Alarms das Wachpersonal am Einsatzort ist, bevor die Eingänge aufgebrochen werden können.
– Wer eine Tür einbaut, die einem Eindringversuch 30 Minuten widerstehen kann, muss sicherstellen, dass ein Einbruchsversuch sofort bemerkt wird und dann innerhalb der 30 Minuten das Wachpersonal vor Ort ist.
– Die Alarmierungen müssen immer wieder geprobt werden.
– Es muss mindestens einmal im Jahr aufbauend auf die Datensicherungen (Backup) das System wiederhergestellt werden. Hierbei ist auch auf eine funktionsfähige Sicherung des Systems zu achten; dies gilt insbesondere für virtuelle Maschinen und deren Konfiguration.
– Sensible Datenbestände sollten verschlüsselt gespeichert werden. Falls es nicht möglich ist, eine ausreichende Reaktionszeit zu erreichen, müssen die Daten verschlüsselt gespeichert werden.
– Soweit als Maßnahme auch eine Videoüberwachung stattfindet, müssen die rechtlichen Rahmenbedingungen beachtet werden. Dazu gehört insbesondere, dass keine Mitarbeiterüberwachung stattfindet.

In Bad Hersfeld hat man nach den Erfahrungen entsprechende Maßnahmen ergriffen. Vor allem wird durch eine Videoüberwachung mit Alarmierung versucht, einen weiteren Diebstahl zu verhindern. Für den Betrieb der Videoanlage habe ich einige datenschutzrechtliche Anforderungen formuliert. Kernpunkt war dabei, dass Bürger beim Besuch des Landratsamtes nicht überwacht werden. Daraus folgten Einschränkungen bei Videoaufzeichnungen hinsichtlich Ort und Zeitpunkt. Die Überwachung sensibler, zutrittskontrollierter Räume, wie z. B. von Serverräumen, ist möglich; sie muss gesondert geregelt werden.

Mit dem Personalrat muss eine Dienstvereinbarung geschlossen werden, wer in welchen Fällen wie auf Aufzeichnungen zugreifen darf.

Ich habe mich vergewissert, dass die Anforderungen umgesetzt sind. Die Sicherungsmaßnahmen haben nun einen besseren Standard als noch Anfang des Jahres.

4.7
Anforderung der Vorlage von Geburtsurkunden durch den Zweckverband Abfallwirtschaft Vogelsbergkreis

Für die Gewährung von Gebührenminderungen können Nachweise über die Anspruchsberechtigungen gefordert werden. Allerdings ist hierbei darauf zu achten, dass für einen Nachweis nur die tatsächlich erforderlichen Daten

angefordert werden und die Bürger ggf. auf verschiedene Möglichkeiten hingewiesen werden.

Verschiedene Anfragen machten mich darauf aufmerksam, dass im Vogelsbergkreis Vergünstigungen für Familien mit Kindern bei der Berechnung von Müllgebühren nur nach der Vorlage von Geburtsurkunden eingeräumt wurden. Erschwerend kam hierbei hinzu, dass die Vorlage der Geburtsurkunden nicht nur von den betroffenen Familien selbst, sondern auch vom Vermieter angefordert wurde, da dieser für die Zahlung der Müllgebühren verantwortlich ist. Auch ein im Internet zur Verfügung gestelltes Formular des Antrags auf Ermäßigung der Müllgebühren forderte für jedes Kind die Vorlage der Kopie der Geburtsurkunde.

Meine Rückfrage bei dem Zweckverband ergab, dass diesem nur die Anzahl der Personen bekannt sind, die auf einem Grundstück gemeldet sind und diese Zahl zur Berechnung der Müllgebühren herangezogen wird. Solange die Anzahl der Bewohner und die tatsächlichen Gebührenpflichtigen übereinstimmen, muss der Vermieter keine weiteren Nachweise vorlegen. Sollen jedoch mögliche Minderungen der Mindestgebühr in Anspruch genommen werden, so sind auch entsprechende Nachweise erforderlich. Die Form des Nachweises spiele hierbei für den Zweckverband keine Rolle, er muss nur eindeutig die Anspruchskriterien nach der Abfallsammlungssatzung dokumentieren. Enthalten Nachweisdokumente Informationen, die für den Zweckverband nicht erforderlich sind, dürfen diese geschwärzt werden. Leider wurden die Betroffenen weder auf dem Antragsformular noch durch die Mitarbeiterinnen und Mitarbeiter des Zweckverbandes auf die verschiedenen Möglichkeiten zur Erfüllung der Nachweispflichten hingewiesen, wie z. B. die Vorlage einer Schulbescheinigung oder einer Meldebescheinigung des Kindes.

Aufgrund meiner Nachfragen hat der Zweckverband inzwischen das Antragsformular geändert und ein Hinweisblatt hinzugefügt, das die verschiedenen Möglichkeiten des Nachweises für eine Minderung der Müllgebühren aufzeigt. Um Missverständnisse sicher auszuschließen, werden inzwischen Nachweise nur noch mit aufwendigeren Schreiben angefordert, die auf die verschiedenen Möglichkeiten hinweisen.

Die Beschwerdeführer habe ich entsprechend informiert. Seit der Umstellung des Verfahrens erreichten mich keine Beschwerden mehr.

5. Aufsichtsbehörde nach § 38 BDSG

5.1
Elektronisches Lastschriftverfahren

Die für die großen Dienstleister (Provider/Netzbetreiber) im elektronischen Lastschriftverfahren zuständigen Datenschutzaufsichtsbehörden haben sich auf einheitliche Richtlinien für eine datenschutzgerechte Ausgestaltung dieses Verfahrens verständigt.

5.1.1
Unterschiede und grundsätzliche Funktionsweise von elektronischem Lastschriftverfahren und Electronic-Cash-Verfahren

Bei der Zahlung mit einer EC-Karte sind die Abläufe beim Electronic-Cash-Verfahren (EC-Cash-Verfahren) und dem elektronischen Lastschriftverfahren (ELV) zu unterscheiden.

Electronic Cash ist ein Karten-System der Deutschen Kreditwirtschaft, der Vertretung der kreditwirtschaftlichen Spitzenverbände Deutschlands. Karten mit dem „electronic cash"-Logo werden nur von Kreditinstituten ausgegeben, üblicherweise in Verbindung mit einem Girokonto. Beim electronic cash erfolgt die Zahlung, indem der Karteninhaber seine PIN (Persönliche Identifikationsnummer) an einem speziellen Lese- und Datenübertragungsgerät (sogenanntes EFT-POS-Terminal, d. h. Electronic-Funds-Transfer-Terminal, Elektronische-Werte-Übertragungs-Terminal) eingibt. Die Bezeichnung EC stammt ursprünglich von Eurocheque, einem europaweiten, einheitlichen Scheckzahlungssystem in Verbindung mit einer Bankgarantie. Ähnliche Karten-Systeme sind Maestro und V Pay (http://de.wikipedia.org/wiki/Ec-cash, Stand 17. Okt. 2011; im Folgenden vereinfachend nur: „EC-Cash-Verfahren"). Die Eingabe der PIN löst eine Online-Überprüfung des Kartenkontos durch die Bank des Betroffenen aus. Bei ausreichender Kontodeckung und Kartengültigkeit wird der Zahlbetrag garantiert und die Zahlung abgewickelt. Dafür verlangen die Banken allerdings von den Händlern eine Gebühr (0,3 % des Umsatzes, mindestens 8 Cent je Transaktion).

Beim elektronischen Lastschriftverfahren hingegen zahlt der Zahlungspflichtige (im Folgenden auch „Kunde" oder „Betroffener" genannt) quasi nur mit seiner Unterschrift.

Es handelt sich um ein Einzugsermächtigungsverfahren, das heißt, der Zahlungsempfänger (Gläubiger der Geldschuld, also Händler, Handwerker, Dienstleister etc., im folgenden vereinfachend: „Händler") wird schriftlich

vom Zahlungspflichtigen ermächtigt, den genannten Zahlungsbetrag vom Girokonto des Zahlungspflichtigen durch Lastschrift einzuziehen (http://de.wikipedia.org/wiki/Lastschrift, Stand 13. Okt. 2011). Dabei wird die Zahlstelle (Bank des Betroffenen) nicht involviert und kann deshalb die formelle und materielle Berechtigung einer Lastschrift nicht prüfen.

Im Gegensatz zum PIN-Verfahren liegt beim ELV also das Risiko, dass das Konto des Käufers nicht gedeckt ist, die Karte ungültig oder gestohlen ist, auf Seiten der Händler. Der Käufer kann beim ELV die Lastschrift ohne Angabe von Gründen widerrufen. (Näheres zu den Lastschriftrückgaben siehe unter Ziff. 5.1.3.3.) Daher trägt der Händler insgesamt das Risiko, dass die Lastschrift „platzt", indem es zu einer Rücklastschrift kommt. Das ELV ist somit für den Händler grundsätzlich riskanter. Gleichwohl wird es von den Händlern vielfach eingesetzt, weil es das kostengünstigere Verfahren ist.

Wenn es zu einer Lastschriftrückgabe kommt, benötigt der Händler den Namen und die Adresse des Käufers, um die offene Forderung beitreiben zu können. Da die Bank diese Daten nur herausgeben darf, wenn der Betroffene hierfür seine Bank vom Bankgeheimnis befreit hat, lassen sich die Händler auf den ELV-Belegen eine entsprechende Anweisung an die Bank unterschreiben. Für die Adressauskunft verlangen die Banken ebenfalls Gebühren.

Sowohl beim EC-Cash als auch beim ELV-Verfahren bedienen sich die Händler meist spezieller Dienstleister für die Zahlungsabwicklung, sogenannter „Netzbetreiber". Die meisten ELV-Netzbetreiber sind zugleich EC-Netzbetreiber. In Hessen haben vier solcher Netzbetreiber ihren Sitz. Weitere große Netzbetreiber sind in Bayern und Nordrhein-Westfalen ansässig. Die in diesen drei Bundesländern ansässigen Netzbetreiber repräsentieren ca. 85–90 % des EC-Kartenumsatzes in Deutschland.

Aufgrund der immer wieder vorkommenden Forderungsausfälle beim ELV haben die Netzbetreiber Systeme zur Vermeidung und Reduzierung dieser Risiken entwickelt (Näheres hierzu siehe Ziff. 5.1.3.3 bis 5.1.3.5). In der Regel gleicht der Netzbetreiber den ihm vom Händler übermittelten Datensatz zu einem Zahlungsvorgang mit den bei ihm gespeicherten Datenbeständen ab und trifft anschließend eine Aussage darüber, ob dem Händler die Zahlung im ELV oder statt dessen nur im Wege des PIN-Verfahrens empfohlen werden kann. Man spricht hier von einer „Zahlungswegeempfehlung". Durch diese Systeme ist das ELV laut Aussagen des Handelsverbandes Deutschland (HDE), der insoweit auf polizeiliche Kriminalstatistiken verweist, ein sicheres Zahlungsmittel geworden.

5.1.2
Datenströme, Anlass der Prüfung und Vorgehensweise der Aufsichtsbehörden

Am Kassenterminal des Händlers werden beim ELV aus der Karte des Kunden insbesondere die Bankleitzahl, die Kontonummer, die Kartenfolgenummer, das Datum des Gültigkeitsablaufs der Karte sowie der Ländercode ausgelesen und zusammen mit Daten der Transaktion (Höhe der Forderung, Datum und Uhrzeit der Zahlung, die Identifikationsnummer des Zahlungsterminals, aus dem sich der Ort der Zahlung ergibt, sowie ggf. eine fortlaufende Nummer für jede Transaktion, die vom Terminal vergeben wird) an den Netzbetreiber zur Zahlungsabwicklung weitergegeben.

Selbstverständlich ist es möglich, dass der Händler die Daten unmittelbar an seine Hausbank übermittelt, damit diese die Lastschrift einzieht. Die Datenverarbeitung ist dann insgesamt nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig, denn sie hält sich im Rahmen dessen, was für die Erfüllung des Vertrages mit dem Kunden erforderlich ist.

§ 28 Abs. 1 BDSG

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

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

Bedient sich der Händler eines Netzbetreibers und beschränkt sich dieser auf die reine Zahlungsabwicklung, so hält sich die Datenverarbeitung ebenfalls im Rahmen des nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG Zulässigen. (Die Datenweitergabe an den Netzbetreiber stellt je nach Ausgestaltung eine Auftragsdatenverarbeitung nach § 11 BDSG dar oder eine Funktionsübertragung, die aber nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist.)

Werden die Daten jedoch vom Netzbetreiber darüber hinaus verwendet, um dem Händler Zahlungswegeempfehlungen (Zahlung mittels ELV oder PIN) zu geben, so ist dies für die Erfüllung des Vertrages zwischen dem Händler und dem Kunden nicht mehr erforderlich. Daher sind solche Datenverarbeitungen und -nutzungen grundsätzlich problematisch und bedürfen jedenfalls einer eigenen Rechtsgrundlage.

Die ELV-Belege sahen bislang vor, dass die Kunden in die Datenverarbeitungen, welche für die Zahlungswegeempfehlung erfolgen, einwilligen und dies unterschreiben. Teilweise war die Einwilligungsklausel mit den entsprechenden Informationen nur auf dem Exemplar des Händlers gedruckt, wurde also dem Kunden nicht überreicht. Das Verfahren rief aus unter-

schiedlichen Gründen die Kritik von Datenschützern hervor. Die Verbraucherzentrale Bundesverband sah Verstöße gegen die Vorschriften über allgemeine Geschäftsbedingungen und forderte von Händlern und Netzbetreibern die Abgabe von Unterlassungserklärungen und erhob gegen einen Händler auch eine Unterlassungsklage.

In Bezug auf einen außerhalb Hessens ansässigen Netzbetreiber gab es Hinweise, dass die Daten aus dem ELV für andere Zwecke als nur für die Zahlungsabwicklung und Zahlungswegeempfehlung genutzt werden sollten (Näheres hierzu unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Pressemitteilungsarchiv/Inhalt/PM_Datenschutz/Inhalt/2011/Easycash/Easycash.php.)

Wenngleich die öffentlich geäußerte Kritik teilweise sehr pauschal war und erhebliche Unterschiede zwischen den Verfahren der verschiedenen Netzbetreiber ebenso unberücksichtigt ließ wie bereits erfolgte Abstimmungen zwischen Netzbetreibern und einzelnen Aufsichtsbehörden (Näheres hierzu unter Ziff. 5.1.3.2), sahen sich die Aufsichtsbehörden im Bundesgebiet veranlasst, die Datenverarbeitungen im Zusammenhang mit dem ELV insgesamt auf den Prüfstand zu stellen. Hierfür gründete der „Düsseldorfer Kreis“ (Abstimmungsgremium der Datenschutzaufsichtsbehörden im Bundesgebiet für den nicht öffentlichen Bereich) im Jahr 2010 eine ad hoc-Arbeitsgruppe „Elektronisches Lastschriftverfahren“. Den Vorsitz übernahm das Bayerische Landesamt für Datenschutzaufsicht (davor bis Juli 2011 die Datenschutzaufsicht bei der Regierung von Mittelfranken). Hessen wurde zunächst durch das Regierungspräsidium Darmstadt und seit dem 1. Juli 2011 durch mich vertreten.

Die großen Netzbetreiber beauftragten einen renommierten Dienstleiter im Bereich Datenschutz und IT-Sicherheit, eine umfassende objektive Darstellung der verschiedenen in der Praxis befindlichen ELV-Verfahren und der damit einhergehenden Datenströme zu erstellen. Diese Untersuchung stellte eine sehr hilfreiche Grundlage für die Abstimmungen dar. Es zeigte sich, dass die ELV-Verfahren sehr vielfältig sind und zum Teil starke Divergenzen bei den einzelnen Netzbetreibern bestanden. Außerdem boten die Netzbetreiber eine ganze Reihe von Zusatzdiensten an. Die Arbeitsgruppe beschränkte sich darauf, das „normale“ ELV zu behandeln.

Es kam indessen zu keiner einheitlichen Bewertung.

Die Aufsichtsbehörden von Hessen, Bayern und Nordrhein-Westfalen sowie eine ganze Reihe weiterer Aufsichtsbehörden haben sich jedoch auf einheitliche Richtlinien für eine datenschutzgerechte Ausgestaltung des ELV verständigt. Diese werden nachfolgend dargestellt.

5.1.3
Rechtliche Bewertung

5.1.3.1
Personenbezogene Daten

Auch wenn der Name des Karteninhabers grundsätzlich nicht erhoben wird (nur bei der Lastschriftrückgabe), so handelt es sich bei den verarbeiteten Zahlungsdaten gleichwohl um personenbezogene Daten, denn sie sind personenbeziehbar. Somit ist das BDSG anwendbar; hierin waren sich alle Aufsichtsbehörden einig.

5.1.3.2
Abkehr von der Einwilligungslösung

Die Lastschriftermächtigungserklärung sowie die Anweisung an die Bank, bei einer Rücklastschrift den Namen sowie die Adresse des Kontoinhabers an den Händler zu übermitteln, standen nicht auf dem Prüfstand der Aufsichtsbehörden. Diese Erklärungen/Einwilligungen sind unzweifelhaft erforderlich und unbedenklich.

Vielmehr ging es nur um die Rechtsgrundlage für die Datenverwendungen, die für die Zahlungswegeempfehlung (ELV oder PIN) erfolgen.

Nach § 4 Abs. 1 BDSG kommt die Einwilligung des Betroffenen als Rechtsgrundlage für diese Erhebung, Verarbeitung und Nutzung personenbezogener Daten in Betracht.

§ 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.

Das BDSG stellt jedoch in § 4a Abs. 1 BDSG hohe Anforderungen an die Wirksamkeit einer Einwilligung.

§ 4a Abs. 1 BDSG

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

Die Einwilligung der Betroffenen kann die Datenverwendungen somit nur rechtfertigen, wenn sie vor der Datenverwendung erfolgt, und zwar grundsätzlich in Schriftform und wenn die Betroffenen ausreichend informiert sind. Das Schriftformerfordernis bedeutet, dass die Betroffenen die Einwilligung eigenhändig unterzeichnen müssen (§ 126 BGB).

Beim ELV besteht jedoch das Problem, dass die Datenverwendungen, die für die Zahlungswegeempfehlung erfolgen, bereits stattgefunden haben, wenn der Betroffene die Einwilligung auf dem Lastschriftbeleg unterschreibt. Diese schriftliche Einwilligung kommt insoweit zu spät. Es stellt sich daher die Frage, ob die Hingabe der Karte zwecks ELV-Zahlung als konkludente Einwilligung gewertet werden kann und ob diese nach § 4a BDSG wirksam ist.

Eine Ausnahme vom Schriftformerfordernis ist nach § 4a Abs. 1 Satz 3 BDSG nur möglich, wenn wegen besonderer Umstände eine andere Form angemessen ist.

Einer der in Hessen ansässigen Netzbetreiber hatte bis zum Jahr 2008 seinen Sitz in einem anderen Bundesland. Im Zeitraum von 2006/2005 prüfte die damals dort zuständige Datenschutzaufsichtsbehörde das Verfahren aufgrund einer Beratungsanfrage des Unternehmens. (Es lässt sich von mir nicht sicher nachvollziehen, ob der Sachverhalt, von dem die Aufsichtsbehörde ausging, in allen relevanten Einzelheiten mit dem Verfahren, wie es im Jahr 2010/2011 betrieben wurde, übereinstimmte.) In ihrer Bewertung erachtete sie eine konkludente Einwilligung durchaus für möglich, allerdings unter der Voraussetzung, dass die Betroffenen beim Händler durch einen Aushang im Kassenbereich die erforderlichen Informationen erhalten, um die Tragweite ihrer Entscheidung verstehen zu können. Der Netzbetreiber verpflichtete demzufolge seine Vertragspartner (Händler) in den allgemeinen Geschäftsbedingungen, einen entsprechenden, mit der damals zuständigen Aufsichtsbehörde abgestimmten Informationstext auszuhängen. Bei der Umsetzung dieser Verpflichtung durch die Händler gab es jedoch erhebliche Defizite.

Meines Erachtens kann durchaus angenommen werden, dass beim ELV besondere Umstände vorliegen. Denn wenn der Betroffene schon vor der Hingabe der Karte gebeten würde, eine Einwilligung zu unterschreiben, müsste er, falls das ELV akzeptiert wird, erneut um seine Unterschrift gebeten werden, und zwar unter der Lastschriftermächtigung und der Anweisung an die Bank, bei Nichteinlösung seinen Namen nebst Anschrift an den Händler zu übermitteln. Dies wäre keine praktikable Lösung. Andererseits wäre es nicht gerechtfertigt, den Betroffenen vorab diese Erklärungen unterschrieben zu lassen, bevor also geklärt ist, ob das ELV überhaupt vom Händler akzeptiert wird.

Gleichwohl ist nicht zu verkennen, dass es zumindest problematisch ist, wenn die Datenverarbeitung auf eine konkludente Einwilligung gestützt werden soll. Es ist bereits streitig, ob überhaupt konkludente Einwilligungen anerkannt werden können (Simitis Bundesdatenschutzgesetz, 7. Auflage, § 4a, Rdnr. 44). Hauptsächlich aber ist fraglich, ob gewährleistet werden kann, dass die hohen Anforderungen an eine informierte Einwilligung (§ 4a Abs. 1 Satz 2 BDSG) erfüllt werden. Die Betroffenen müssen vor der Einwilligung alle Informationen erhalten, die notwendig sind, um Anlass, Ziel und Folgen der Datenverarbeitung korrekt abzuschätzen (Simitis, § 4a Rdnr. 70). Ist dies nicht sichergestellt, so ist die Datenverarbeitung unzulässig.

Die nach § 4a Abs. 1 Satz 1 BDSG erforderliche Freiwilligkeit der Einwilligung kann zweifelhaft sein, wenn ein Händler kein PIN-Verfahren als Alternative zum ELV anbietet. Die Barzahlung dürfte jedenfalls nicht immer als eine zumutbare Alternative empfunden werden.

Insgesamt ist es also mit nicht unerheblichen Risiken behaftet, wenn die Datenverarbeitung auf eine (konkludente) Einwilligung gestützt wird.

Daher wurde den Netzbetreibern empfohlen, von der Einwilligungslösung abzukehren. (Zu den Besonderheiten beim ELV im Internet siehe unter Ziff. 5.1.4.) Die Datenverarbeitungen sollten auf das beschränkt werden, was nach den gesetzlichen Erlaubnistatbeständen zulässig ist (s. hierzu Näheres unter Ziff. 5.1.3.3 bis 5.1.3.6).

5.1.3.3
Abgleich mit KUNO-Datei

KUNO steht für die Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen. Es handelt sich um ein freiwilliges System der Polizeibehörden und der Wirtschaft. Ziel ist es, Betrugsfälle im kartengestützten Zahlungsverkehr zu reduzieren.

Wenn ein Betroffener den Verlust seiner EC-Karte bei seiner Bank meldet und die Karte bei der Bank sperren lässt, so ist die Karte – wie sich bereits aus obigen Ausführungen ergibt – damit noch nicht für das Lastschriftverfahren gesperrt. Die Karte kann vom Dieb oder Finder missbräuchlich eingesetzt werden. Um dies zu verhindern, wurde KUNO etabliert. Der Karteninhaber sollte die Karte auch bei der Polizei als gestohlen (oder verloren) melden. Die Polizei meldet dann die Daten der abhanden gekommenen Debitkarte (Bankleitzahl, Kontonummer und Kartenfolgenummer) einem Kooperationspartner des Einzelhandels. Von dort werden diese Daten an die dem KUNO-Sperrsystem angeschlossenen Einzelhandelsgeschäfte

bzw. an die Netzbetreiber weitergeleitet. Durch den Abgleich mit dieser Sperrdatei kann die Karte auch für das Lastschriftverfahren gesperrt werden. (Näheres zu KUNO unter https://www.kuno-sperrdienst.de.)

Die Speicherung und entsprechende Nutzung dieser KUNO-Sperrdatei ist für die Wahrung berechtigter Interessen der Händler erforderlich und liegt auch im Interesse der Betroffenen. Sie ist somit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. soweit der Netzbetreiber dies vornimmt, nach § 29 Abs. 1 Nr. 1 BDSG zulässig. Näheres zur Einstufung der Netzbetreiber siehe unter Ziff. 5.1.3.6.

§ 28 Abs. 1 Satz 1 BDSG

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

1. *…*
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.*

§ 29 Abs. 1 Nr. 1 BDSG

Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. *kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat.*

5.1.3.4
Abgleich mit Daten über Lastschriftrückgaben

Im Regelfall sind beim Lastschriftverkehr mindestens zwei Kreditinstitute eingeschaltet. Deshalb bedurfte es homogener Regelungen der Kreditinstitute untereinander, wie der Lastschriftverkehr abgewickelt werden soll. Das ist mit dem „Abkommen über den Lastschriftverkehr“ (kurz: Lastschriftabkommen) erstmals im Jahr 1963 geregelt worden, das durch die Spitzenverbände der deutschen Kreditwirtschaft und der Deutschen Bundesbank geschlossen wurde und dem alle Sparkassen, Volksbanken und Geschäftsbanken beigetreten sind.

Eine nicht eingelöste Lastschrift wird als Lastschriftrückgabe bezeichnet. Sie wird nach einem im Lastschriftabkommen definierten Verfahren zwischen den beteiligten Banken zurückgerechnet, dem Konto des Zahlungsempfängers wieder belastet und dem Konto des Zahlungspflichtigen wieder gutgeschrieben. Beim ELV kann es folgende Gründe für die Rückgabe einer Lastschrift geben:

– Das Einzugskonto weist keine Deckung auf, das heißt, dass auf dem Konto weder ausreichendes Guthaben vorhanden ist noch eine ausreichende Kreditlinie besteht.
– Das angegebene Konto (bzw. die Karte) besteht nicht oder ist aufgelöst worden, die Karte ist also ungültig.
– Der Zahlungspflichtige hat der Lastschrift widersprochen. (Ein solcher Widerspruch/Widerruf muss nicht begründet werden.)

Bankgebühren für Lastschriftrückgaben darf die Zahlstelle aufgrund verschiedener Urteile des Bundesgerichtshofs vom Zahlungspflichtigen nicht verlangen (Urteil vom 8. März 2005, Az. XI ZR 154/04). Entgelte für den Einreicher der Lastschrift sind dagegen zulässig (http://de.wikipedia.org/wiki/Lastschrift, Stand 13. Oktober 2011).

Die Erstellung einer Sperrdatei aus den Daten solcher Lastschriftrückgaben und deren Nutzung für eine Zahlungswegeempfehlung ist für die Wahrung der berechtigten Interessen der Händler erforderlich. Schutzwürdige Belange der Betroffenen stehen grundsätzlich nicht entgegen, sofern die Daten aus der Sperrdatei gelöscht werden, wenn die Forderung doch noch erfüllt wurde.

Es spielt keine Rolle, ob die Lastschriftrückgabe bei demselben Händler erfolgt ist, bei dem der Betroffene nun erneut mittels ELV bezahlen will oder ob die Lastschriftrückgabe bei einem anderen Händler erfolgte. Die Daten können also auch händlerübergreifend verwendet werden.

Ausnahmsweise können jedoch die schutzwürdigen Belange der Betroffenen entgegenstehen. Ein solcher Fall läge vor, wenn die gekaufte Ware Sachmängel aufweist oder der Betroffene die Ware gar nicht erhalten hat und er deshalb die Zahlung rückgängig macht, indem er die Lastschrift widerruft. Im stationären Handel kommt es jedoch bei einem Sachmangel nur sehr selten zu einem Lastschriftwiderruf. Vielmehr begibt sich der Betroffene in der Regel in das Ladengeschäft, wo der Umtausch der Ware oder die Rücküberweisung des Kaufpreises erfolgt. Im Versandhandelsbereich kann es jedoch eher vorkommen, dass Betroffene die Lastschrift widerrufen, um ihre Rechte aus dem Kaufvertrag geltend zu machen.

Es wäre nicht gerechtfertigt, wenn ein Betroffener, der die Lastschrift aus gutem Grund widerrufen hat, vom ELV ausgeschlossen würde.

Daher müssen die Händler und Netzbetreiber sicherzustellen, dass Daten aus solchen Rücklastschriften, bei denen der Betroffene durch den Widerruf der Lastschrift erklärtermaßen Rechte aus dem der Lastschrift zu Grunde liegenden Geschäft geltend macht, nicht in die händlerübergreifende Sperrdatei einbezogen werden.

Unter dieser Voraussetzung ist die Datenverarbeitung ebenfalls nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. soweit der Netzbetreiber dies vornimmt, nach § 29 Abs. 1 Nr. 1 BDSG zulässig.

(Zu den Transparenzanforderungen siehe unter Ziff. 5.1.3.7.)

5.1.3.5
Abgleich mit Zahlungsdaten, bei denen keine Lastschriftrückgaben vorliegen („Positivdaten“)

Verständlicherweise möchten Händler einen möglichen Missbrauch des ELV auch in den Fällen vermeiden, in denen es noch keine Auffälligkeiten gab, also weder ein Eintrag in der KUNO-Sperrdatei vorhanden ist noch eine Lastschriftrückgabe vorliegt. Der Missbrauchserkennung dient beispielsweise die sogenannte Entfernungsprüfung: Hier erkennen die Datenverarbeitungssysteme, ob die Kartendaten innerhalb eines begrenzten Zeitfensters an zwei weit entfernten Orten in Deutschland verwendet werden. Das Zeitfenster wird so gewählt, dass ein Einsatz derselben Karte an den weit entfernten Orten nicht möglich ist. Anhand dieser Prüfung ergeben sich also sehr starke Indizien für den Einsatz gefälschter Karten.

Umfassendere Auswertungen der Zahlungsdaten können ebenfalls dazu dienen, Indizien für einen möglichen Missbrauch des ELV zu erhalten, oder um sonstige Interessen der Netzbetreiber oder Händler zu verfolgen.

Die gebotene Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG bzw. nach § 29 Abs. 1 Nr. 1 BDSG führt zu einer differenzierten Bewertung:

Die Bildung eines händlerübergreifenden Pools mit Positivdaten, die aus Zahlungen mittels elektronischen Lastschriftverfahrens stammen, ist auf gesetzlicher Grundlage datenschutzrechtlich zulässig, soweit die Daten ausschließlich zur Missbrauchsbekämpfung im Elektronischen Lastschriftverfahren verwendet und nach einer kurzen Zeit – höchstens einigen wenigen Tagen – aus dem Pool gelöscht werden. (Die Löschpflicht besteht nur, soweit nicht gesetzliche Aufbewahrungspflichten entgegenstehen.)

Die Speicherung und Nutzung von Positiv- und Rücklastschriftdaten, die aus Zahlungen mittels ELV im Rahmen eigener Kundenkontakte des Händlers stammen, kann außer für Zwecke der Missbrauchsbekämpfung auch für die Steuerung einer Limitgewährung (Limitsteuerung) und der Verhinderung von Zahlungsausfällen im Elektronischen Lastschriftverfahren nach den genannten Vorschriften zulässig sein. Hierfür können auch Zahlungsdaten aus einem längeren Zeitraum als nur einigen wenigen Tagen verwendet werden. Beispielsweise könnte ein Händler vorgeben, dass das ELV nur

eingesetzt wird, wenn verschiedene Einkäufe mit einer Karte in einem Zeitraum von 30 Tagen einen Betrag von 400 Euro nicht übersteigen. Über welchen Zeitraum maximal eine Auswertung erfolgen darf, muss noch definiert werden.

Eine darüber hinausgehende Speicherung und Nutzung für andere Zwecke – insbesondere zur Profilbildung – kann aber nicht auf die genannte Rechtsgrundlage gestützt werden.

Bei dem Begriff „Händler“, welcher bei der dargestellten differenzierten Bewertung maßgeblich ist, ist auf die jeweilige juristische Person abzustellen. Rechtlich selbständige Unternehmen, die zur gleichen Unternehmensgruppe gehören oder in sonstiger Weise wirtschaftlich zusammenarbeiten, stellen datenschutzrechtlich eigenständige verantwortliche Stellen dar. Die Abwägung mit den schutzwürdigen Belangen der Betroffenen rechtfertigt es nicht, diese als Einheit zu behandeln.

In jedem Fall (unabhängig davon, ob es sich um Daten eines einzelnen Händlers oder mehrerer Händler handelt) unzulässig wäre es, die Daten mit weiteren Daten zusammenzuführen, die mit ganz anderer Zwecksetzung erhoben wurden, beispielsweise mit Daten aus Kundenbindungsprogrammen.

Auch eine Zusammenführung mit Daten aus dem EC-Cash-Verfahren wäre nicht gerechtfertigt. Ebenso wenig wäre eine Datenübermittlung an Auskunfteien nach den o. g. Vorschriften zulässig. Dies gilt auch für die Daten aus Lastschriftrückgaben (siehe Ziff. 5.1.3.4).

5.1.3.6
Rolle der Netzbetreiber, unzulässige Verarbeitungen

Die rechtliche Einordnung der Tätigkeit der Netzbetreiber und damit der Datenweitergabe an diese ist jeweils zu klären. Je nach konkreter Ausgestaltung kann eine Auftragsdatenverarbeitung gemäß § 11 BDSG oder aber eine Datenübermittlung mit nachfolgender eigenverantwortlicher Datenverarbeitung und -nutzung vorliegen.

Soweit ein Netzbetreiber händlerübergreifende Auswertungen vornimmt, handelt es sich um eine auskunfteienähnliche Tätigkeit, auf die § 29 BDSG anwendbar ist.

Die Übermittlung von aus dem ELV stammenden Positiv- oder Rücklastschriftdaten durch Netzbetreiber an Händler unabhängig von einer aktuellen ELV-Transaktion („auf Vorrat“) zum Zwecke einer möglichen Verwendung zu einem späteren Zeitpunkt ist unzulässig. Dies gilt auch für die Übermittlung von bloßen Zahlungswegeempfehlungen nebst den betreffenden Kartendaten. Auch an solchen Daten hat der Händler erst dann ein berechtigtes Interesse, dem die schutzwürdigen Belange der Betroffenen nicht entgegenstehen, wenn die konkrete Karte beim jeweiligen Händler für das ELV vorgelegt wird. Lediglich die KUNO-Daten dürfen auf Vorrat übermittelt werden, denn die Betroffenen haben ein Interesse daran, dass die Daten den Händlern auf jeden Fall zur Verfügung stehen.

5.1.3.7
Transparenzanforderungen

Bei der Datenerhebung müssen die Transparenzanforderungen des § 4 Abs. 3 Satz 1 BDSG erfüllt werden.

§ 4 Abs. 3 BDSG

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.

Verantwortlich sind hierfür die Händler. Insbesondere muss über die oben aufgeführten Zwecke der Datenverarbeitung sowie die Weitergabe bzw. Übermittlung an Netzbetreiber unterrichtet werden. Dies kann durch einen Aushangtext an der Kasse erfolgen sowie durch eine Kurzfassung der Informationen auf dem Belegtext. Auf Wunsch sollten den Betroffenen nähere Informationen zur Verfügung gestellt werden, zum Beispiel an der Kasse, beim Filialleiter und/oder im Internet.

In der Arbeitsgruppe ELV wurden Beispiele für entsprechende Aushang- und Belegtexte erarbeitet. Im Einzelnen können auch gleichwertige andere Formulierungen verwendet werden. Vor allem muss je nach eingesetztem Verfahren geprüft werden, ob die Texte anzupassen sind. Die Beispieltexte berücksichtigen lediglich die datenschutzrechtlichen Anforderungen. Da die Datenschutzaufsichtsbehörden keine Zuständigkeit im AGB-Recht besitzen, müssten derartige Anforderungen daher zusätzlich von den Unternehmen in Eigenverantwortung geklärt werden.

Die Aufsichtsbehörden Bayern, Nordrhein-Westfalen und Hessen haben vereinbart, bei den im jeweiligen Bundesland ansässigen ELV-Netzbetreibern für die Umsetzung der Informationstexte (ggf. nach inhaltlicher Anpas-

sung) zu sorgen. Die Netzbetreiber müssen die letztlich zu verwendenden Textinhalte den angeschlossenen Unternehmen zur Kenntnis bringen und vertraglich dafür sorgen, dass diese Texte verwendet werden.

Dementsprechend habe ich alle in Hessen ansässigen Netzbetreiber informiert. Die bisherigen Abstimmungen haben gezeigt, dass die Netzbetreiber insgesamt als verantwortliche Stellen für die von ihnen durchgeführten Datenverarbeitungen einzustufen sind. Dies muss daher im Aushangtext ergänzt werden. Ferner ist in den Texten der Begriff „übermitteln“ statt „weitergeben“ bzgl. des Datentransfers vom Händler an den Netzbetreiber zu verwenden.

5.1.4
Sonderthemen, weiteres Vorgehen

Für das Internet gelten spezielle Regelungen. Hier ist beim ELV die Übermittlung von Positiv- oder Rücklastschriftdaten an Netzbetreiber sowie die Verarbeitung und Nutzung durch Netzbetreiber nach § 12 Abs. 1 und Abs. 2 Telemediengesetz (TMG) jeweils nur mit Einwilligung zulässig, denn das Telemediengesetz enthält keine Rechtsgrundlage für diese Datenverarbeitungen.

§ 12 TMG

(1) Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

(2) Der Diensteanbieter darf für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

Die Einholung einer rechtswirksamen Einwilligung ist bei Bezahlung mittels Elektronischen Lastschriftverfahren im Internet grundsätzlich möglich. Die Aufsichtsbehörden beabsichtigen, auch hierfür entsprechende Beispieltexte abzustimmen.

In der Arbeitsgruppe ELV wird auch noch abschließend zu bewerten sein, ob und inwieweit Besonderheiten gelten, wenn der Netzbetreiber im Wege der Vorausabtretung die Forderungen gegen die Endkunden pauschal oder aufschiebend bedingt für den Fall der Lastschriftrückgabe erwirbt.

Im Zusammenhang mit den Initiativen zur Etablierung eines einheitlichen Euro-Zahlungsverkehrsraums, in dem alle Zahlungen wie inländische Zahlungen behandelt werden (Single European Payment Area – SEPA), wurden europäische Lastschriftverfahren entwickelt. Welche Auswirkungen die SEPA-Vorgaben auf das ELV haben, bleibt abzuwarten. Es wird dann zu untersuchen sein, welche datenschutzrechtlichen Konsequenzen sich für das ELV ergeben.

Beispieltext für einen ELV-Beleg

Ich ermächtige
das oben / umseitig genannte **U**….. (Name des Unternehmens) sowie den **N**….. (Name des Netzbetreibers), den heute fälligen, umseitigen Betrag von meinem Konto per Lastschrift einzuziehen.

Ich weise mein Kreditinstitut unwiderruflich an,
bei Nichteinlösung der Lastschrift dem **U**….. (und/oder dem **N**…..) auf Anforderung meinen Namen und meine Anschrift zur Geltendmachung der Forderung mitzuteilen.

(UNTERSCHRIFT)

Datenschutzrechtliche Information
Meine Zahlungsdaten (Kontonummer, Bankleitzahl, Kartenverfallsdatum, Kartenfolgenummer, Datum, Uhrzeit, Zahlungsbetrag, Terminalkennung, Ort, Unternehmen und Filiale) werden zur Kartenprüfung und Zahlungsabwicklung an (den Dienstleister) **N**….. weitergegeben.

An **N**….. wird ferner gemeldet, wenn eine Lastschrift mangels Deckung nicht eingelöst oder von Ihnen widerrufen wurde (Rücklastschrift), außer wenn Sie im Zusammenhang mit dem Widerruf erklärtermaßen Rechte aus dem zugrundeliegenden Geschäft (z. B. wegen eines Sachmangels bei einem Kauf) geltend gemacht haben.

Zudem werden die Zahlungsdaten **zur Verhinderung von Kartenmissbrauch** und gemeinsam mit den Rücklastschriftdaten **zur Begrenzung des Risikos von Zahlungsausfällen** gespeichert und genutzt. **N**….. erteilt insoweit auch an andere Händler, die an seinem System angeschlossen sind, Empfehlungen, ob eine Zahlung mit EC-Karte und Unterschrift akzeptiert werden kann.

Beispieltext für einen Aushang

Kundeninformation zur Zahlung mit EC-Karte und Unterschrift in Zusammenarbeit mit N….. (Name Netzbetreiber)

Wir leiten folgende Zahlungsinformationen – ohne Namen – an N….. weiter:

– Ihre Kontonummer und Bankleitzahl, das Kartenverfallsdatum und die Kartenfolgenummer Ihrer EC-Karte;
– Datum, Uhrzeit, Betrag der Zahlung, Terminal-Kennung (Ort, Unternehmen und Filiale).

Diese Daten werden zur Prüfung und Durchführung Ihrer Zahlung benötigt. Darüber hinaus dienen sie zur Verhinderung von Kartenmissbrauch und zur Begrenzung des Risikos von Zahlungsausfällen. Dazu sind Höchstbeträge für Zahlungen innerhalb bestimmter Zeiträume festgelegt. Die von U… (Name des Unternehmens) verwendeten Höchstbeträge sind grundsätzlich für alle EC-Karten gleich. / U….. kann für unterschiedliche EC-Karten unterschiedliche Höchstbeträge festlegen.[1]

An N….. wird auch gemeldet, wenn eine Lastschrift von Ihrer Bank mangels Deckung nicht eingelöst oder von Ihnen widerrufen wurde (Rücklastschrift), außer wenn Sie im Zusammenhang mit dem Widerruf erklärtermaßen Rechte aus dem zugrunde liegenden Geschäft (z. B. wegen eines Sachmangels bei einem Kauf) geltend machen. Dies dient zur Verhinderung künftiger Zahlungsausfälle. Sobald die Forderung beglichen wird, wird die Meldung gelöscht.

Mit Hilfe dieser Informationen kann N….. an Händler, die an seinem System angeschlossen sind, Empfehlungen für ihre Entscheidung erteilen, ob sie eine Zahlung mit EC-Karte und Unterschrift akzeptieren wollen. N….. kann zu diesem Zweck

– Rücklastschriftinformationen von allen bei ihm angeschlossenen Händlern verwenden;
– für eine kurze Zeit – wenige Tage – zur Verhinderung von Kartenmissbrauch Zahlungsinformationen auch händlerübergreifend auswerten (verwenden);
– darüber hinaus nur solche Zahlungsinformationen auswerten (verwenden), die er vom selben Händler erhalten hat.

Eine Nutzung Ihrer Daten *für Bonitätszwecke/zum Zweck der Bonitätsprüfung*[2] findet nicht statt. Ihre Zahlungsdaten werden ausschließlich für die Entscheidung darüber genutzt, ob dem jeweiligen Händler eine Zahlung mit EC-Karte und Unterschrift empfohlen wird.

Nähere Informationen erhalten Sie auf Wunsch an der Kasse.

[1] Je nach der Gestaltung im konkreten Fall soll hier der eine oder aber der andere Satz (bzw. gleichwertige Formulierungen) zum Einsatz kommen.
[2] Alternativmögliche Formulierungen.

5.2
Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Als Reaktion auf eine Vielzahl von Datenschutzskandalen wurde die Vorschrift des § 42a BDSG geschaffen. Sie trat am 1. September 2009 in Kraft und verpflichtet Unternehmen, bei bestimmten, als besonders kritisch eingestuften Datenverlusten oder „Datenpannen“ sowohl die Datenschutzaufsichtsbehörde als auch die Betroffenen zu informieren. Die bisherigen Erfahrungen zeigen, dass sich die Vorschrift trotz einiger Auslegungsfragen grundsätzlich bewährt hat.

§ 42a BDSG wurde durch Artikel 1 Nummer 16 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009 (BGBl. I S. 2814) in das Bundesdatenschutzgesetz eingefügt. Danach müssen Vorfälle, bei denen bestimmte personenbezogene Daten unrechtmäßig an Dritte übermittelt oder in sonstiger Weise Dritten zur Kenntnis gelangt sind, unverzüglich der zuständigen Aufsichtsbehörde gemeldet werden. Ferner sind die Betroffenen zu informieren. Die Verpflichtung besteht unabhängig davon, ob das Unternehmen die unrechtmäßige Kenntniserlangung durch Dritte verschuldet hat. Sie greift jedoch nur, wenn die Daten unter die in Satz 1 der Vorschrift aufgeführten Datenkategorien fallen. Weitere Voraussetzung für die Informationspflicht ist, dass für die Rechte oder schutzwürdigen Interessen der Betroffenen schwerwiegende Beeinträchtigungen drohen.

§ 42a BDSG

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. *besondere Arten personenbezogener Daten (§ 3 Absatz 9),*
2. *personenbezogene Daten, die einem Berufsgeheimnis unterliegen,*
3. *personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder*
4. *personenbezogene Daten zu Bank- oder Kreditkartenkonten*

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen

Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Adressaten dieser Regelung sind nicht-öffentliche Stellen (§ 2 Abs. 4 BDSG), d. h. natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht Aufgaben der öffentlichen Verwaltung oder hoheitliche Aufgaben wahrnehmen, oder Vereinigungen von öffentlichen Stellen des Bundes oder der Länder sind. Aufgrund des Verweises in § 42a Satz 1 BDSG auf § 27 Abs. 1 Satz 1 Nr. 2 BDSG müssen auch öffentliche Stellen des Bundes, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, § 42a BDSG beachten. Öffentliche Stellen des Landes Hessen, die als Wettbewerbsunternehmen tätig sind, werden dadurch erfasst, dass das Hessische Datenschutzgesetz in § 3 Abs. 6 partiell auf das Bundesdatenschutzgesetz und somit auf § 42a BDSG verweist. Daher haben beispielsweise die Sparkassen § 42a BDSG zu beachten.

§ 3 Abs. 6 HDSG

Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der zweite Teil sowie die §§ 34 und 36 dieses Gesetztes. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

Für sonstige öffentliche Stellen des Bundes und der Länder ist § 42a BDSG nicht anwendbar.

Anderes gilt allerdings für die dem § 42a BDSG entsprechenden Informationspflichten nach § 93 Abs. 3 Telekommunikationsgesetz (TKG). Dort wird keine Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen getroffen. Die Vorschrift gilt für alle Anbieter von Telekommunikationsdiensten.

§ 93 Abs. 3 TKG

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestandsdaten oder Verkehrsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

Auch für die Anbieter von Telemedien bestehen nach § 15a Telemediengesetz (TMG) entsprechende Informationspflichten, unabhängig davon, ob es sich um nicht-öffentliche oder öffentliche Stellen handelt.

§ 15a TMG

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

Aufgrund der Regelungen in § 93 Abs. 3 TKG und § 15a TMG werden die Informationspflichten also auf Vorfälle erweitert, bei denen dem TKG oder dem TMG unterfallende Datenarten betroffen sind. Damit wird quasi der in § 42a Satz 1 BDSG aufgeführte Katalog der relevanten Datenkategorien ausgedehnt.

Auftragsdatenverarbeiter nach § 11 BDSG sind nicht Adressaten des § 42a BDSG. Gemäß § 11 Abs. 4 BDSG gelten für den Auftragnehmer nur bestimmte Vorschriften des BDSG. § 42a BDSG wird in § 11 Abs. 4 BDSG nicht erwähnt. Für einen Verlust von Daten, die beim Auftragnehmer im Auftrag gespeichert waren, ist der Auftraggeber verantwortlich. Die Benachrichtigungspflicht ist von ihm wahrzunehmen. Kommt es hier zu Verzögerungen oder unterlassenen Meldungen, bleibt dies dem Auftraggeber anzulasten. Der Auftraggeber hat deshalb dafür Sorge zu tragen, dass der Auftragnehmer zur unverzüglichen Meldung ihm gegenüber verpflichtet ist. Der Vertrag nach § 11 BDSG muss entsprechende Regelungen enthalten. Die vom Regierungspräsidium Darmstadt entworfene Mustervereinbarung zur Auftragsdatenverarbeitung nach § 11 BDSG sieht hierzu folgende Formulierung vor:

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42a BDSG. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach § 42a BDSG zu unterstützen.

Wie bereits oben ausgeführt, bestehen die Informationspflichten nach § 42a BDSG nur, wenn Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Unrechtmäßig ist eine Übermittlung oder sonstige Kenntniserlangung durch Dritte, wenn keine Zustimmung der Betroffenen vorliegt und die Offenbarung weder durch das Gesetz noch eine sonstige Rechtsvorschrift erlaubt ist.

Die Kenntniserlangung durch einen Dritten muss nicht sicher festgestellt werden. Es ist ausreichend, wenn es entweder offensichtlich ist, dass Dritte Kenntnis erlangt haben, oder wenn anhand von tatsächlichen Anhaltspunkten mit einer gewissen Wahrscheinlichkeit hiervon ausgegangen werden kann. Eine Informationspflicht kommt auch in Fällen des Datenverlustes in Betracht. So z. B. wenn Laptops, USB-Sticks oder andere Datenträger an Orten verloren gehen, wo sie Dritten zugänglich und die Daten nicht verschlüsselt sind. Von einer Kenntniserlangung ist auch bei einem Diebstahl auszugehen, wenn die Daten nicht oder nur unzureichend verschlüsselt waren.

Da für die Auslösung der Informationspflicht zusätzlich noch das Drohen von schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen hinzukommen muss, ist jeder Fall sorgfältig zu prüfen und zu würdigen. Es ist jeweils eine Prognose zu erstellen, mit der die Wahrscheinlichkeit schwerwiegender Beeinträchtigungen bewertet wird. Der Bundesrat hatte im Gesetzgebungsverfahren gefordert, die Worte „und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ zu streichen [BTDrucks. 16/12011, Seite 45 (Anlage 3 Nummer 19)]. Diesem Antrag ist der Gesetzgeber nicht gefolgt. Die Bundesregierung hatte in ihrer Gegenäußerung den Bundesratsvorschlag abgelehnt und hierbei u. a. ausgeführt, dass Konstellationen denkbar seien, in denen diese Daten Dritten unrechtmäßig zur Kenntnis gelangen, ohne dass hieraus eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen droht, z. B. wenn die Daten verschlüsselt waren [BTDrucks. 16/12011, Seite 52 (Anlage 4, zu Nummer 19)].

Bei einer Verschlüsselung kann es indes bereits an der Kenntniserlangung durch Dritten fehlen, sofern es sich um eine starke Verschlüsselung handelt.

Das Beispiel der Bundesregierung zeigt nach meiner Auffassung jedenfalls, dass der Maßstab, wann diese zusätzliche Voraussetzung (drohende schwerwiegende Beeinträchtigung) vorliegt, nicht zu hoch anzulegen ist.

Bei den seit dem 1. September 2009 in Hessen gemeldeten Fällen handelte es sich mehrheitlich um Diebstahldelikte. Bei diesen Fällen waren Datenträger mit Daten zu Bankverbindungen, Kontonummern etc. entwendet worden. Das Vorliegen der Voraussetzungen des § 42a BDSG wurde von der Aufsichtsbehörde überprüft und in den meisten Fällen bejaht. In einem Fall wurde eine Informationspflicht nach der vom verantwortlichen Unternehmen vorgelegten Risikoanalyse als nicht gegeben angesehen, da die Rekonstruktion einzelner Daten aus dem entwendeten Gesamtbestand nur unter einem sehr hohen technischen Aufwand, der in keiner Relation zu den dadurch entschlüsselten Daten gestanden hätte, möglich gewesen wäre.

Bei Diebstählen hat sich die Aufsichtsbehörde in allen Fällen die Anzeige bei den polizeilichen Ermittlungsstellen in Kopie zusenden lassen.

Die zweite größere Fallgruppe waren Fehlversendungen oder Verlust oder Teilverlust auf dem Postweg. Da hier auch Kontendaten möglicherweise an unberechtigte Dritte übermittelt wurden und schwerwiegende Folgen für die Betroffenen bei einem solchen Verlust nach Auffassung der Aufsichtsbehörde grundsätzlich immer eintreten können, wurde von der Aufsichtsbehörde die Informationspflicht in diesen Fällen bejaht.

Die Verpflichtung zur Information der Aufsichtsbehörde hat zu einer Vielzahl von Meldungen geführt, die die Aufsichtsbehörde in Kenntnis und in die Lage gesetzt haben, in konkreten Einzelfällen Maßnahmen für die Zukunft zu empfehlen. Diese gingen von Maßnahmen zur physischen Sicherung von eingesetzten Laptops in Arztpraxen bis zur Empfehlung von Verschlüsselungen und Zugriffsbeschränkungen auf den Datenbestand bei mobilen Diensten.

Generell lässt sich sagen, dass jeder Fall nach § 42a BDSG als Einzelfall zu sehen ist und sowohl das Bestehen der Informationspflichten als auch die zu treffenden Maßnahmen im Einzelfall zu prüfen sind.

Erfreulicherweise haben Unternehmen auch in Fällen, in denen nicht eindeutig geklärt war, ob die Voraussetzungen des § 42a BDSG tatsächlich vorlagen, sowohl die Betroffenen als auch die Aufsichtsbehörde oder zumindest die Aufsichtsbehörde benachrichtigt. Verantwortlichen Stellen ist sehr zu empfehlen, mich auch künftig in Zweifelsfällen zu informieren.

Verstöße gegen § 42a BDSG können nach § 43 Abs. 2 Ziffer 7 BDSG mit einem Bußgeld bis zu 50.000 Euro geahndet werden. Unter bestimmten Voraussetzungen kann dieser Bußgeldrahmen sogar überschritten werden.

Der Aufsichtsbehörde wurden seit Inkrafttreten dieser Neuregelung allerdings – bis auf eine Ausnahme, bei der die verantwortliche Stelle eine irrige Rechtsauffassung vertreten hatte – keine Fälle bekannt, in denen eine klar zu bejahende Informationspflicht nicht erfüllt wurde.

Eine vom BfDI durchgeführte bundesweite Erhebung bei den Datenschutzaufsichtsbehörden ergab, dass in den ersten 18 Monaten nach Inkrafttreten der Informationspflichten insgesamt fast 90 Fälle, hiervon in Hessen 24 Fälle, gemeldet wurden. Dies kann durchaus als Beleg gewertet werden, dass die Pflicht (auch in Hessen) ernst genommen wird. Wie hoch die Dunkelziffer ist, vermag ich allerdings nicht zu beurteilen.

Eine Aufstellung der seit Inkrafttreten der Vorschrift bis zum 31. Dezember 2011 gemeldeten Fälle steht am Ende dieses Beitrags.

Nicht nur über die Fallzahlen, sondern auch über die Auslegung der Vorschrift tauschen sich die Aufsichtsbehörden aus. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit hat Hinweise in Form von FAQs zur Identifizierung der mitteilungspflichtigen Sachverhalte und zur Umsetzung der Handlungspflichten veröffentlicht (http://www.datenschutz-berlin.de/attachments/809/535.4.7.pdf?1311923219).

§ 48 BDSG verpflichtet die Bundesregierung, dem Bundestag zum 31. Dezember 2012 über die Auswirkungen des § 42a BDSG zu berichten. Nach bisherigen Erfahrungen kann die Vorschrift aus meiner Sicht als sinnvoll bewertet werden.

Eine Harmonisierung auf europäischer Ebene sollte angestrebt werden. Hierzu gibt es auch bereits Ansätze:

Die revidierte Datenschutzrichtlinie für elektronische Kommunikation legt erstmals in der EU einen Rahmen für eine Verpflichtung zur Anzeige von Verstößen gegen die Datenschutzvorschriften fest. Dieser Rahmen findet nur auf die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung, z. B. Anbieter von Kommunikationsnetzen und Internetzugangsanbieter (Artikel 2 der Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, „Rahmenrichtlinie“).

Im Zusammenhang mit der Überprüfung der EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Nr. 96/46 könnte auch auf europarechtlicher Ebene eine sektorübergreifende Regelung erfolgen. Die EU-Kommission beabsichtigt eine Prüfung der Modalitäten für die Einführung einer Anzeigepflicht bei Datenschutzverstößen in der allgemeinen Datenschutzregelung, die alle Sektoren abdeckt und mit der Anzeigepflicht gemäß der Datenschutzrichtlinie für elektronische Kommunikation übereinstimmen sollte (s. Seiten 6–7 der Mitteilung der Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“, KOM(2010) 609 endgültig vom 4. November 2010).

Die Artikel 29-Datenschutzgruppe begrüßt dies, da sie davon überzeugt ist, dass sektorübergreifende Meldungen von Sicherheitsverletzungen dem Einzelnen helfen, die notwendigen Schritte für eine Begrenzung des möglichen, aus der Verletzung resultierenden Schadens zu unternehmen. Außerdem geht die Artikel 29-Datenschutzgruppe davon aus, die Anzeigepflicht werde Unternehmen dazu anhalten, für mehr Datensicherheit zu sorgen, und ihre Rechenschaftspflicht stärken (s. Arbeitspapier 184 der Artikel 29-Datenschutzgruppe, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_de.pdf).

Ich teile diese Einschätzung. Durch einheitliche europäische Vorgaben würden auch grenzüberschreitende Vorfälle besser erfasst und Wettbewerbsnachteile für deutsche Unternehmen vermieden.

Übersicht über die Meldungen nach § 42a BDSG in Hessen

Anzahl der eingegangenen Meldungen insgesamt: 40

Informationspflicht nach § 42a BDSG bejaht: 36

	Anlass der Meldung	Informationspflicht
1	Verschwinden von 2 Metallkoffern mit Bankunterlagen	Ja
2	Diebstahl eines Computers aus einer Arztpraxis	Ja
3	Diebstahl eines Laptops (Gesundheitsdaten)	Ja
4	Fehlversendung Bankunterlagen	Ja
5	Fehlversendungen mit Kontodaten	Ja
6	Laptopdiebstahl (mit Daten über pflegebedürftige Personen)	Ja
7	Einbruchdiebstahl (Entwendung von Mitgliederlisten mit Bankverbindungen)	Ja
8	Entwendete Patientenadressliste	Ja
9	Verlust von Mitarbeiterdaten auf dem Postweg (Bankdaten)	Ja

	Anlass der Meldung	Informationspflicht
10	Sicherheitslücke, die es ermöglicht hat, in fremde E-Mails Einsicht zu nehmen	Ja
11	Datendiebstahl bei Kreditkartenpersonalisierer	Ja, nach Abschluss der staatsanwaltlichen Ermittlungen
12	Fehlversendungen von Bankdaten	Ja
13	Übermittlung von Mitarbeiter- und Kundendaten an eigene Mailadresse	Nein, Übermittlung an eigene Person und an den Rechtsanwalt zur Wahrnehmung prozessrechtlicher Vertretung
14	Vorübergehender Verlust von Bankdaten (verschlossener Koffer)	Nein, Koffer wurde kurz nach Verlust unversehrt bei der Polizei abgegeben
15	Fehlversendung Jahressteuerbescheinigungen	Ja
16	Zugriff auf Daten mit Bankverbindungen durch ein Zugangsleck im Internetauftritt	Ja
17	Entwendung einer Chipkarte mit Bildern von Teilen von Personen aus dem Bereich der Mammographie	Nein, Bilder nicht Personen zuzuordnen
18	Verlust von Mitarbeiterdaten auf dem Postweg (Bankdaten, Versicherungen, Religion)	Ja
19	Fehlversendung von Bankunterlagen	Ja
20	Fehlversendung einer Eigenauskunft (mit Kontodaten)	Ja
21	Fehlerhaft ausgehändigte Kontenübersicht	Ja
22	Fehlversand von Bankunterlagen	Ja
23	Fehlversendung einer Eigenauskunft (Kontodaten)	Ja
24	Verlust eines Paketes mit Mitarbeiterdaten (Abrechnungsunterlagen)	Ja

	Anlass der Meldung	Informationspflicht
25	Illegale Erhebung von Namen und Mailadressen anlässlich eines „Hackerangriffes“ auf eine Versandfirma	Nein, nachweisbar keine Daten des § 42a BDSG betroffen
26	Verlust eines USB-Sticks auf dem Postweg	Ja
27	Aushändigung von Kontoauszügen an einen unberechtigten Dritten	Ja
28	Diebstahl eines Laptops aus einer Arztpraxis	Ja
29	Fehlversand von Eigenauskünften einer Auskunftei	Ja
30	Fehlgeleitetes Fax mit Kontounterlagen	Ja
31	Diebstahl von Kundendaten	Ja, nach vorgelegter Risikoanalyse und in Anbetracht der Tatsache, dass die Daten verschlüsselt waren, wurde eine Informationspflicht der Betroffenen im konkreten Einzelfall nicht gesehen.
32	Einbruchdiebstahl (Entwendung von Überweisungsaufträgen, Schecks und sonst. Schriftstücken)	Ja
33	Einbruchdiebstahl (Entwendung von Überweisungsaufträgen, Schecks und sonst. Schriftstücken)	Ja
34	Verlust von neuen Kundenbankkarten auf dem Postweg, anschl. missbräuchliche Verfügungen zu Ungunsten dieser Kunden	Ja
35	Skimming-Vorfall, anschl. u. a. missbräuchliche Verfügungen aus z. B. Kenia, Chile, USA, insgesamt 12 unberechtigte Buchungen mit Schaden i. H. v. ca. 9.300 Euro	Ja
36	Fehlerhafte Zugriffsregelung anlässlich konzernweiter Umstellung auf SAP	Ja

	Anlass der Meldung	Informationspflicht
37	Einbruchsdiebstahl (Entwendung eines Laptops mit Kreditkartendaten von Kunden)	Ja
38	Unberechtigter Zugriff bzw. Kenntniserlangung (Hackerangriff) von Kundendaten (Kreditkarten und PayPal) auf einen Web-Shop	Ja
39	Internetzugriffe auf Personal- bzw. Bewerberdaten im Firmenintranet aufgrund mangelhafter Schutzmaßnahmen	Ja
40	Versehentlicher Fehlversand von Telefaxen (Krankenversichertenunterlagen)	Ja

Stand: 31.12.2011

6. Entwicklungen und Empfehlungen im Bereich der Technik

6.1
Orientierungshilfe „Cloud-Computing“

Die Orientierungshilfe „Cloud-Computing“ der Datenschutzbeauftragten des Bundes und der Länder ist unter Federführung meines Hauses erstellt worden. Sie beleuchtet neben technischen auch rechtliche Aspekte.

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich bereits seit längerer Zeit mit der Thematik des Cloud-Computing. Da das Thema immer mehr an Aktualität gewinnt, wurde von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und des Düsseldorfer Kreises die vorliegende Orientierungshilfe unter Federführung meines Hauses erarbeitet. Um nicht nur technische, sondern vor allen Dingen auch rechtliche Aspekte beleuchten zu können, wurden hierbei die Arbeitsgruppen Telemedien und Internationaler Datenverkehr des Düsseldorfer Kreises eingebunden. Die Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern. Sie konnte nicht die Unterschiede der Datenschutzgesetze in Bund und Ländern berücksichtigen, weshalb als Grundlage der rechtlichen Ausführungen das Bundesdatenschutzgesetz diente. Deshalb sind die rechtlichen Aussagen unmittelbar nur auf den nicht öffentlichen Bereich und die Bundesverwaltung anwendbar.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sie zustimmend zur Kenntnis genommen. Die aktuelle Fassung ist auf meiner Homepage veröffentlicht (http://www.datenschutz.hessen.de/ft-oh_technik.htm).

Die Orientierungshilfe ist wie folgt aufgebaut:

Kapitel 1 führt in das Thema ein. Cloud-Computing steht für vielfältige Möglichkeiten, Dienstleistungen zur Datenverarbeitung unter Verwendung des Internet oder anderer Wide Area Networks wie Konzernnetze oder die Landesnetze der Verwaltungen in Anspruch zu nehmen. Ob Public, Private, Community oder Hybrid Clouds, ob Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastructure as a Service (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.

In **Kapitel 2** werden rund um das Cloud-Computing die wichtigsten Begriffe erläutert. Leider besteht in der Praxis keine einheitliche Terminologie. Daher haben sich die Definitionen an den Ausführungen des BSI und des Fraunhofer Institutes für Offene Kommunikationssysteme orientiert. Die Beschreibungen für Cloud-Anbieter und Cloud-Anwender, die Basisinfrastrukturen Public Cloud, Private Cloud und Community Cloud und die Betriebsmodelle SaaS, PaaS 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 Auswirkungen auf die Betroffenenrechte auseinander. Weiter wird der grenzüberschreitende Datenverkehr beleuchtet. Hierbei muss zwischen dem innereuropäischen und dem außereuropäischen Raum unterschieden werden. Die Orientierungshilfe gibt Empfehlungen zum datenschutzgerechten Einsatz. Besonders hilfreich sind die Musterverträge auf meiner Homepage (www.datenschutz.hessen/ft-auftragverarbeit.htm).

Kapitel 4 beschäftigt sich mit den technischen und organisatorischen Maßnahmen. Cloud-Computing-Systeme der Cloud-Anbieter unterliegen bestimmten infrastrukturellen Rahmenbedingungen, deren Schutz bezüglich der Grundwerte Verfügbarkeit, Vertraulichkeit, Integrität, Revisionssicherheit und Transparenz (nähere Definitionen siehe Kapitel 4.1.1) gewährleistet werden muss.

Dieser Schutz orientiert sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten. Die Umsetzung der Schutzziele ist durch technische und organisatorische Maßnahmen abzusichern.

Kapitel 4.1.2 beschreibt die grundsätzlichen cloud-spezifischen Risiken. In Kapitel 4.1.3 werden die klassischen Risiken, die ein Erreichen der Schutzziele in der Cloud zusätzlich erschweren, näher erläutert.

In den nachfolgenden Kapiteln 4.2 bis 4.4 werden anhand der beschriebenen Schutzziele für die verschiedenen Betriebsmodelle IaaS, PaaS, SaaS die Risiken differenziert und nochmals spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

Kapitel 5 zieht ein Fazit. 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 des Risikos von Unterkapazitäten einerseits und der Kosten für die Vorhaltung von Reservekapazitäten andererseits sowie die bessere Planbarkeit der Kosten der Datenverarbeitung sind für Unternehmen und Behörden 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 Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können;
- transparente, detaillierte und eindeutige vertragliche Regelungen der cloud-gestützten Datenverarbeitung, 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;
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

6.2
Attribute/Attribut-Zertifikate bei der dienstlichen Nutzung der qualifizierten Signatur

Immer wieder erreichen mich Anfragen zur dienstlichen Nutzung der qualifizierten elektronischen Signatur. Dabei geht es neben der Frage, welche

personenbezogenen Daten hierfür erhoben werden dürfen, auch darum, wann eine Signatur dienstlich ist und wann nicht und ob und wie mit der dienstlich eingesetzten Signatur die „jederzeitige Erkennbarkeit der Identität der Person“ sichergestellt werden kann. Hier leistet das Attribut im Signaturzertifikat bzw. ein eigenes Attribut-Zertifikat einen wichtigen Beitrag, der noch viel zu wenig bekannt ist.

6.2.1
Einführung

Inzwischen gibt es zwei bundesweite Verfahren, bei denen die bisherige Verarbeitung mit Papier durch eine ausschließlich elektronische unter Verwendung qualifizierter elektronischer Signaturen ersetzt wurde: das elektronische Personenstandsregister (ePR) und das elektronische Abfallnachweisverfahren (eANV). Letzteres befindet sich noch bis 31. Januar 2012 in der Übergangsphase. Bei diesem Verfahren sind außer Behörden auch Firmen beteiligt, für die die weiteren Ausführungen im Wesentlichen analog gelten.

Bei der dienstlichen Verwendung von Signaturen stellen sich zwei Fragen: Welche Möglichkeiten gibt es, eine Vertretungsmacht für Dritte oder berufsbezogene (und sonstige) Angaben zur Person des Antragstellers mit einer qualifizierten elektronischen Signatur zu verbinden? Und wie kann man sie bei Bedarf, bspw. bei (fristloser) Kündigung, Beurlaubung oder einstweiligem Ruhestand, auch schnellstmöglich wieder entfernen?

Da die qualifizierte elektronische Signatur der handschriftlichen Unterschrift gleichgestellt ist, steht sie zunächst einmal grundsätzlich nur dem Signaturschlüsselinhaber persönlich zur Verfügung.

6.2.2
Attribute und Attribut-Zertifikate

Das Signaturgesetz lässt in § 5 Abs. 2 SigG aber mit dem „Attribut“ einen Weg zu, wie auf Verlangen des Antragstellers eine Vertretungsmacht für Dritte oder berufsbezogene (und sonstige) Angaben in die Signatur integriert werden können. Dessen Inhalt bedarf der Einwilligung der dritten Person bzw. der Bestätigung durch die für die berufsbezogenen oder sonstigen Angaben zuständigen Stelle (z. B. Arbeitgeber, Rechtsanwalts- oder Ärztekammer). Auch die Anforderungen an die Nachweise bzw. Bestätigungen sind in diesem Absatz im Einzelnen genannt.

§ 5 Abs. 2 SigG

Ein qualifiziertes Zertifikat kann auf Verlangen eines Antragstellers Angaben über seine Vertretungsmacht für eine dritte Person sowie berufsbezogene oder sonstige Angaben zu seiner Person (Attribute) enthalten. Hinsichtlich der Angaben über die Vertretungsmacht ist die Einwilligung der dritten Person nachzuweisen; berufsbezogene oder sonstige Angaben zur Person sind durch die für die berufsbezogenen oder sonstigen Angaben zuständige Stelle zu bestätigen. Angaben über die Vertretungsmacht für eine dritte Person dürfen nur bei Nachweis der Einwilligung nach Satz 2, berufsbezogene oder sonstige Angaben des Antragstellers zur Person nur bei Vorlage der Bestätigung nach Satz 2 in ein qualifiziertes Zertifikat aufgenommen werden. Weitere personenbezogene Angaben dürfen in ein qualifiziertes Zertifikat nur mit Einwilligung des Betroffenen aufgenommen werden.

Das Signaturgesetz bietet zwei verschiedene Varianten für die Unterbringung eines solchen Attributes an: Sie können entweder direkt in das Signatur-Zertifikat aufgenommen werden (§ 7 Abs. 1 Nr. 9 SigG) oder in ein „gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat)“ (§ 7 Abs. 2 SigG).

§ 7 SigG

(1) Ein qualifiziertes Zertifikat muss folgende Angaben enthalten und eine qualifizierte elektronische Signatur tragen:

1. *den Namen des Signaturschlüssel-Inhabers, der im Falle einer Verwechslungsmöglichkeit mit einem Zusatz zu versehen ist, oder ein dem Signaturschlüssel-Inhaber zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muss,*
2. *den zugeordneten Signaturprüfschlüssel,*
3. *die Bezeichnung der Algorithmen, mit denen der Signaturprüfschlüssel des Signaturschlüssel-Inhabers sowie der Signaturprüfschlüssel des Zertifizierungsdiensteanbieters benutzt werden kann,*
4. *die laufende Nummer des Zertifikates,*
5. *Beginn und Ende der Gültigkeit des Zertifikates,*
6. *den Namen des Zertifizierungsdiensteanbieters und des Staates, in dem er niedergelassen ist,*
7. *Angaben darüber, ob die Nutzung des Signaturschlüssels auf bestimmte Anwendungen nach Art oder Umfang beschränkt ist,*
8. *Angaben, dass es sich um ein qualifiziertes Zertifikat handelt, und*
9. *nach Bedarf Attribute des Signaturschlüssel-Inhabers.*

(2) Attribute können auch in ein gesondertes qualifiziertes Zertifikat (qualifiziertes Attribut-Zertifikat) aufgenommen werden. Bei einem qualifizierten Attribut-Zertifikat können die Angaben nach Absatz 1 durch eindeutige Referenzdaten des qualifizierten Zertifikates, auf das sie Bezug nehmen, ersetzt werden, soweit sie nicht für die Nutzung des qualifizierten Attribut-Zertifikates benötigt werden.

Das Attribut-Zertifikat stellt die Verbindung zum eigentlichen Signatur-Zertifikat her, das die Rolle eines Basis-Zertifikates hat und den Signaturprüfschlüssel enthält. Wegen dieser inhaltlichen Abhängigkeit gilt es auch

höchstens so lange wie das Signatur-Zertifikat, auf das es sich bezieht. Es kann bei Bedarf in die Signatur einbezogen werden. Mit einem dienstlichen Attribut-Zertifikat handelt es sich dann um eine dienstliche, ohne seine Einbindung um eine private Signatur.

Das Attribut-Zertifikat kann separat gesperrt und beantragt werden. Das ist in der Regel wesentlich kostengünstiger als ein Wechsel in Form von Sperrung eines alten und Ausstellung eines neuen Basis-Zertifikates, weil es ohne Erzeugung eines neuen Signaturschlüsselpaares auskommt. Da in den meisten Fällen keine neuen Signaturschlüssel auf vorhandene Signaturkarten nachgeladen werden dürfen oder können, wird mit der Nutzung von Attribut-Zertifikaten in diesen Fällen sogar die Ausstellung einer neuen Signaturkarte vermieden.

Über weitere Felder in den existierenden technischen Standards (z. B. Common PKI, X.509) für Signatur- und Attribut-Zertifikate lassen sich die Rechte der Nutzenden zusätzlich gezielt einschränken und erweitern.

6.2.2.1 Einfluss des Attributgebers

Das Signaturgesetz sieht verschiedene Voraussetzungen für die Sperrung von qualifizierten Zertifikaten vor.

Mit der Aufnahme eines Attributes in ein Signatur- oder Attribut-Zertifikat wird der dritten Person bzw. der zuständigen Stelle in § 8 Abs. 2 SigG gleichzeitig auch die Möglichkeit eingeräumt, das zugehörige Zertifikat jederzeit zu widerrufen bzw. seine Sperrung zu beantragen, wenn die Voraussetzungen nicht mehr gegeben sind.

Andere Sperrmöglichkeiten bestehen nach § 8 Abs. 1 SigG nur auf Verlangen des Signaturschlüsselinhabers, bei falschen Angaben im Zertifikat, wenn der Zertifizierungsdienstanbieter (ZDA) seine Tätigkeit beendet und sie nicht von einem anderen ZDA übernommen wird oder wenn die BNetzA das als Aufsichtsmaßnahme nach § 19 Abs. 4 SigG anordnet. Bei Letzterem geht es um Fälschungen und Fälschungssicherheit. Somit hat ein Arbeitgeber bzw. eine Behörde genau dann Einfluss auf die weitere Nutzung eines Zertifikates, wenn er bzw. sie ein Attribut(-Zertifikat) vergeben hat und die berufsbezogenen (oder sonstigen) Angaben entfallen.

Die Sperrung darf nicht rückwirkend erfolgen (§ 8 Abs. 1 Satz 4 SigG), sonst könnte man bereits geleistete Signaturen bei Bedarf nachträglich für ungültig erklären. Dies stünde im Widerspruch zur erforderlichen Rechtssicherheit und Rechtsverbindlichkeit für den elektronischen Geschäftsverkehr. Die

Sperrung kann aber schon im Vorhinein mit Angabe des Sperrzeitpunktes erfolgen (§ 8 Abs. 1 Satz 3 SigG).

§ 8 SigG

(1) Der Zertifizierungsdiensteanbieter hat ein qualifiziertes Zertifikat unverzüglich zu sperren, wenn ein Signaturschlüssel-Inhaber oder sein Vertreter es verlangt, das Zertifikat auf Grund falscher Angaben zu § 7 ausgestellt wurde, der Zertifizierungsdiensteanbieter seine Tätigkeit beendet und diese nicht von einem anderen Zertifizierungsdiensteanbieter fortgeführt wird oder die zuständige Behörde gemäß § 19 Abs. 4 eine Sperrung anordnet. Weitere Sperrungsgründe können vertraglich vereinbart werden. Die Sperrung muss den Zeitpunkt enthalten, von dem an sie gilt. Eine rückwirkende Sperrung ist unzulässig. Wurde ein qualifiziertes Zertifikat mit falschen Angaben ausgestellt, kann der Zertifizierungsdiensteanbieter dies zusätzlich kenntlich machen.

(2) Enthält ein qualifiziertes Zertifikat Angaben nach § 5 Abs. 2, so kann auch die dritte Person oder die für die berufsbezogenen oder sonstigen Angaben zur Person zuständige Stelle, wenn die Voraussetzungen für die berufsbezogenen oder sonstigen Angaben zur Person nach Aufnahme in das qualifizierte Zertifikat entfallen, eine Sperrung des betreffenden Zertifikates nach Absatz 1 verlangen.

6.2.2.2 Formulierung der Attribute

Sinnvoll wäre eine einheitliche Handhabung beim Aufbau und der konkreten Formulierung der Attribute für alle behördlichen Signaturen. So könnte festgelegt werden, ob stets zuerst die Behördenbezeichnung – ggf. in einer kurzen, sprechenden Form – und danach die konkrete Rolle oder Tätigkeit, bspw. „Urkundsbeamtin“, der Signaturschlüsselinhaberin eingetragen wird oder in umgekehrter Reihenfolge. Auch Trennzeichen zwischen den Bestandteilen können vorgegeben werden.

Damit könnte die automatisierte Prüfung solcher Signaturen erheblich vereinfacht und beschleunigt werden. Es wäre hilfreich, wenn hier schnell eine behördenübergreifende einheitliche Regelung gefunden würde, die sich formal an den vorhandenen technischen Standards orientiert. Dabei wäre auch zu klären, wo und wie eine solche Regelung rechtlich verankert werden kann.

6.2.3 Eindeutige Identifizierbarkeit

Ein anderes Thema ist die eindeutige Identifizierbarkeit oder die jederzeitige Feststellbarkeit der Identität der Signierenden.

Wie die Datenschutzbeauftragten des Bundes und der Länder immer wieder betont haben, muss zwischen den Funktionen Signatur und Authentisierung klar unterschieden und stets die zutreffende Funktion verwendet werden. Da es sich bei der qualifizierten Signatur um ein Äquivalent zur handschriftlichen Unterschrift handelt, hat der Gesetzgeber bewusst weder Geburtsdatum und -ort noch die Anschrift in das Zertifikat aufgenommen. Sie sind auch der handschriftlichen Unterschrift nicht zu entnehmen. Das Zertifikat enthält nur den Vor- und den Nachnamen (oder ein Pseudonym, das dann als solches gekennzeichnet ist) und gegebenenfalls einen unterscheidenden Zusatz bei Namensgleichheit innerhalb der von einem Zertifizierungsdiensteanbieter vergebenen Zertifikate.

Derzeit wird die Frage diskutiert, ob und wie die Identität der signierenden Person, bspw. bei Beurkundungen, jederzeit erkennbar ist.

Diese Erkennbarkeit muss nicht unbedingt über das Zertifikat selbst oder den ausstellenden Zertifizierungsdiensteanbieter gewährleistet werden. Vielmehr kann und muss die Behörde, wenn ein Attribut gesetzt ist, die eindeutige Identifizierbarkeit der Person jederzeit gewährleisten (u. a. bei Namensgleichheit). Nur so kann sie erforderlichenfalls das zutreffende Basis- oder Attribut-Zertifikat sperren.

Nach meinem Kenntnisstand sind in Hessen die im ePR gespeicherten Dokumente mit Attribut bzw. Attribut-Zertifikaten signiert, sodass die Stadt bzw. das Standesamt feststellbar sind. Insofern ist es möglich, über eine Nachfrage bei der zugehörigen Behörde festzustellen, um welche Person es sich genau handelt.

Da die Signatur- und Attribut-Zertifikate bei der Prüfung der Signatur und vor allem beim Ausdruck der Dokumente meist gar nicht oder zumindest nicht vollständig mit ausgedruckt werden, ist es wegen der einfacheren Handhabbarkeit unbedingt zu empfehlen, zusätzlich die erforderlichen Angaben zur Person auch in das elektronische Dokument selbst aufzunehmen – vor der Anbringung der qualifizierten Signatur. Dies ist nach den Regelungen des Hessischen Verwaltungsverfahrensgesetzes (HVwVfG) zwar nicht erforderlich, denn nach § 3a Abs. 2 besteht die „elektronische Form“ aus dem elektronischen Dokument und der qualifizierten Signatur. Sie beinhaltet also weder den Namen noch die Funktion oder die Behörde der Signierenden. Gleichwohl würden diese Angaben die Handhabung der Dokumente für alle Beteiligten erleichtern. Darüber hinaus sind auch hier bereichs- oder verfahrensspezifische Festlegungen denkbar und wünschenswert, um eine einheitliche Handhabung bezüglich Namens- und Funktionsangaben sowie Behördenzugehörigkeit in der elektronischen Form analog zum Attribut(-zertifikat) der qualifizierten Signatur zu erreichen. Damit ließe sich dann auch die eindeutige Identifizierbarkeit der Person vereinfachen. Dies entspricht im Übrigen auch der Handhabung bei Papierdo-

kumenten, bei denen die Unterschrift regelmäßig durch die Namensangabe ergänzt wird. Einen ersten Schritt in diese Richtung findet man – für einen anderen Regelungsbereich – bereits in § 126a BGB, wo die elektronische Form immerhin den Namen enthält: sie umfasst das elektronische Dokument, den Namen und die qualifizierte Signatur des Ausstellers.

Diese Angaben im Dokument selbst sollten die Vergabe von Attributen aber nicht ersetzen. Denn in diesem Fall hätte die Behörde keine Möglichkeit, das Signatur- bzw. das Attribut-Zertifikat zu sperren. Sie müsste dann einen anderen Weg finden, um die Erstellung einer entsprechenden dienstlichen elektronischen Form durch die betreffende Person schnell, dauerhaft und zuverlässig zu verhindern. Da elektronische Kopfbögen sich leicht speichern und den dienstlichen Festlegungen entsprechend auch von ehemals Berechtigten oder Dritten unberechtigt und unkontrolliert nutzen lassen, scheint das kaum realistisch und jedenfalls viel aufwendiger als das Sperren eines Attributes oder Attribut-Zertifikates.

6.2.4
Fazit und Ausblick

Soweit es um die elektronische Form und damit um wichtige elektronische Dokumente in Behörden (und Unternehmen) geht, scheint die Verwendung von dienstlichen Attributen bzw. Attribut-Zertifikaten unabdingbar, wenn und soweit die Behörde eine missbräuchliche Nutzung dienstlicher Signaturen wirksam und unkompliziert verhindern will oder muss. In diesem Fall ist es dann auch möglich, über eine Nachfrage bei der zugehörigen Behörde festzustellen, um welche Person es sich genau handelt.

Eine einheitliche Handhabung beim Aufbau und der Formulierung der Attribute für jedes Verfahren, das mit der elektronischen Form arbeitet, besser noch: übergreifend für alle behördlichen Signaturen, ist wünschenswert bzw. unter Wirtschaftlichkeitsaspekten erforderlich. Dies kann die Prüfung solcher Signaturen ggf. erheblich vereinfachen. Eine zusätzliche Aufnahme dieser Angaben in die elektronische Form erleichtert den Umgang mit den Dokumenten für alle Beteiligten.

6.3
Anforderungen an ein Datenschutzmanagementsystem – Aufbau und Zertifizierung

Im Rahmen der Diskussion über die Aufgaben der beabsichtigten Stiftung Datenschutz wird auch das Datenschutzaudit diskutiert. Dieses ist zwar seit

langem in § 9a BDSG vorgesehen, die Regelung der Anforderungen, die in einem separaten Gesetz erfolgen sollte, steht aber immer noch aus. Das hat eine Reihe von Unternehmen, die in diesen Bereichen als Dienstleister tätig werden möchten, veranlasst, über die Zertifizierung von Datenschutzmanagementsystemen einerseits und Produkten und Anwendungsverfahren andererseits nachzudenken. Der Beitrag stellt grundsätzliche Überlegungen zu Datenschutzmanagementsystemen vor, beschreibt eine sinnvolle Vorgehensweise und dient dazu, Missverständnisse auszuräumen.

6.3.1
Grundsätzliche Überlegungen

6.3.1.1
Datenschutz, IT-Sicherheit und IT-Grundschutz

Der **Datenschutz** legt fest, unter welchen Voraussetzungen (Rechtsgrundlage, Erforderlichkeit, Zweckbindung, Datenvermeidung etc.) personenbezogene Daten unter Einhaltung bestimmter technischer und organisatorischer Maßnahmen verarbeitet werden dürfen. In Hessen geschieht dies auf der Basis des HDSG für hessische öffentliche Stellen bzw. des BDSG für hessische öffentliche Stellen soweit sie am Wettbewerb teilnehmen und für nicht-öffentliche Stellen. Viele dieser Maßnahmen dienen auch der IT-Sicherheit.

Die **IT-Sicherheit** trifft technische und organisatorische Maßnahmen, um das von einer Organisation (Behörde, Unternehmen) benötigte Maß an Vertraulichkeit, Verfügbarkeit und Integrität der zu verarbeitenden Daten – unabhängig vom Personenbezug – sicherzustellen.

Der Datenschutz betrachtet die Maßnahmen der IT-Sicherheit als wesentliches Werkzeug, um die Datenschutzziele zu erreichen. Zwar sind in den Datenschutzgesetzen unterschiedliche Formulierungen gewählt (z. B. in § 10 Abs. 2 HDSG und Anlage zu § 9 BDSG Zutritts-, Benutzer-, Zugriffs-, Datenverarbeitungs-, Verantwortlichkeits-, Auftrags-, Dokumentations- und Organisationskontrolle; in § 9 ThürDSG oder § 10 DSG NRW Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Revisionsfähigkeit und Transparenz), für das Ergebnis spielt dies jedoch keine Rolle.

Die Betrachtung der Datenschutzziele macht deutlich, dass es trotz unterschiedlichem Fokus im Zeitalter der automatisierten bzw. elektronischen Datenverarbeitung Datenschutz ohne IT-Sicherheit nicht geben kann. Vielmehr umfassen die Maßnahmen für den Datenschutz im Wesentlichen die-

jenigen für die IT-Sicherheit. Als mögliche Ausnahmen seien hier Blitzschutz und Handfeuerlöscher genannt, die man aber durchaus auch als Maßnahmen zur Datenverarbeitungskontrolle bzw. zur Verfügbarkeit sehen kann.

Zur Umsetzung der IT-Sicherheit für Daten mit normalem Schutzbedarf dient der **IT-Grundschutz**. Hier hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Grundschutzkataloge entwickelt, in denen Gefährdungen und zugehörige Maßnahmen für verschiedene Bausteine aufgelistet sind. Diese Kataloge werden ständig aktualisiert und ergänzt.

Es herrscht Einigkeit, dass Datenschutz die Umsetzung des IT-Grundschutzes bei der für die Datenverarbeitung verantwortlichen Stelle und ggf. bei deren Auftragnehmer erfordert bzw. voraussetzt. Denn ein Angreifer wird alle Schwachstellen in der IT einer Organisation für seine Zwecke nutzen, nicht nur jene, die evtl. ausschließlich personenbezogene Daten betreffen.

Es gibt einige Bereiche, in denen Anforderungen und Maßnahmen des Datenschutzes und solche der IT-Sicherheit nicht von vornherein übereinstimmen, sondern erst in Einklang gebracht werden müssen: beispielsweise bei der Protokollierung von externen Angriffen oder Benutzer- und Systemverhalten. Für die IT-Sicherheit wäre eine vollständige Protokollierung aller Aktivitäten über große Zeiträume unbedenklich, datenschutzgerecht ist eine aussagefähige, aber datensparsame Gestaltung der Protokollierung unter Beachtung der Grundsätze der Erforderlichkeit und der Zweckbindung.

Diese gestalterische Aufgabe kann nur gelöst werden, wenn man beide Aspekte gleichzeitig betrachtet. Aus diesem Grund hat der Arbeitskreis Technische und organisatorische Fragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder das IT-Grundschutzhandbuch bzw. die Grundschutzkataloge um den Baustein „B1.5 Datenschutz“ ergänzt, der 13 typische zusätzliche Gefährdungen im Umfeld des Datenschutzes betrachtet und für diesen Bereich ein ergänzendes Maßnahmenbündel von 16 Maßnahmen benennt und ausführlich erläutert, das für alle IT-Systeme und IT-Verfahren anzuwenden ist, mit deren Hilfe personenbezogene Daten verarbeitet werden.

Wegen der oft schwierigen Rechtslage bei Datenschutzfragen in allgemeinen oder spezialrechtlichen Regelungen sollte zur Beurteilung der gesetzlichen Anforderungen und der daraus folgenden Maßnahmen für das IT-Sicherheits- und das Datenschutzkonzept fachkundige Unterstützung in Anspruch genommen werden.

Der Datenschutzbaustein ist in der Zertifizierung nach IT-Grundschutz nicht enthalten, kann aber ggf. von entsprechend qualifizierten Auditoren mit einbezogen werden.

Dies ändert allerdings nichts daran, dass die Einhaltung der datenschutzrechtlichen Bestimmungen durch unabhängige Datenschutz-Kontrollinstanzen überprüft wird:

Die **betrieblichen und behördlichen Datenschutzbeauftragten** haben die Aufgabe der internen Datenschutzkontrolle.

Der **Hessische Datenschutzbeauftragte** ist zuständig für die Beratung und Kontrolle der Dienststellen der hessischen Gebietskörperschaften sowie derjenigen Stellen, die deren Aufsicht unterliegen und Aufgaben der öffentlichen Verwaltung wahrnehmen. Seit dem 1. Juli 2011 ist ihm auch die Aufgabe der Datenschutzaufsichtsbehörde nach § 38 BDSG für die nicht öffentlichen Stellen (z. B. Unternehmen) mit Sitz in Hessen übertragen.

Wenn eine Zertifizierung vorliegt, die die Maßnahmen zum Datenschutz einbezogen hat, kann sie den Aufsichtsbehörden ihre Tätigkeit erleichtern. Das führt – darauf sei an dieser Stelle ausdrücklich hingewiesen – nicht dazu, dass die Datenschutzbeauftragten an das Ergebnis der Zertifizierung gebunden sind; sie können eigene Wertungen treffen.

6.3.1.2 Datenschutzmanagementsystem und Informationssicherheitsmanagementsysteme

Die internationale Norm ISO/IEC 27001 *“Information technology – Security techniques – Information Security Management Systems – Requirements”* spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen (z. B. Handelsunternehmen, staatliche Organisationen, Non-Profit Organisationen) berücksichtigt. Sie beschreibt unter Verwendung des sogenannten “Plan-Do-Check-Act (PDCA)”-Modells einen prozessorientierten Ansatz zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS).

Ein Spezialfall von ISO 27001 ist der BSI-Standard *„ISO 27001 auf der Basis von IT-Grundschutz“*.

Das BSI ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit. Es ist zur Erteilung von Sicherheitszertifikaten für informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile ermächtigt gemäß §§ 3 und 9 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG).

Bei der Zertifizierung nach *„ISO 27001 auf der Basis IT-Grundschutz“* hält sich das BSI an die dafür vorgegebenen internationalen Standards. Dies betrifft neben der Zertifizierung von ISMS gemäß ISO 27001 auch die Akkreditierung der für das BSI in diesem Bereich als Auditoren tätigen Personen gemäß ISO 27006 *“Information technology – Security techniques. Requirements for bodies providing audit and certification of information security management systems”*. Zusätzlich bindet es die Grundschutzkataloge in das Verfahren ein und erreicht damit eine starke Strukturierung, die bei der Durchführung hilfreich sein kann.

Die vom BSI in diesem Bereich vergebenen Zertifikate sind allerdings – im Gegensatz zu den genuinen ISO 27001-Zertifizierungen – nicht international anerkannt. Das hat folgenden Grund: In Deutschland wird die Akkreditierung von Konformitätsbewertungsstellen für ISMS gemäß ISO 27001 als hoheitliche Aufgabe des Bundes durch die Akkreditierungsstelle gemäß § 1 des Gesetzes über die Akkreditierungsstelle (Akkreditierungsstellengesetz – AKKStelleG) durchgeführt. Die deutsche Akkreditierungsstelle führt ein Verzeichnis der akkreditierten Konformitätsbewertungsstellen mit Angabe des fachlichen Umfangs und hält es gemäß § 2 Satz 2 AKKStelleG auf dem neuesten Stand.

Das BSI als nationale Zertifizierungsbehörde im Bereich der IT hat sich nicht selbst dem Verfahren zur Akkreditierung als Konformitätsbewertungsstelle unterworfen.

Der Begriff *„ISO 27001 auf der Basis IT-Grundschutz“* sollte nicht missverstanden werden. Hier werden die Grundschutzkataloge als „Basis“ verwendet. Das bedeutet aber nicht, dass die Zertifizierung nach ISO 27001 auf den Bereich des normalen Schutzbedarfs beschränkt ist oder reduziert wird. Vielmehr ist hier, genauso wie bei der genuinen ISO 27001-Zertifizierung, in jedem Fall eine Risikoanalyse erforderlich. Diese Risikoanalyse ist die Grundlage für die Erstellung der beiden für die Durchführung der Zertifizierung zentralen Dokumente, nämlich des Sicherheitskonzepts und des Risikobehandlungsplans.

Im Falle der Verarbeitung von Daten mit hohem oder sehr hohem Schutzbedarf muss eine „erweiterte“ Risikoanalyse vorgenommen und festgestellt werden, ob und ggf. wie diesen Risiken mit zusätzlichen Maßnahmen so weit begegnet werden kann, dass das Restrisiko tragbar ist. Das gilt zunächst unabhängig davon, ob es sich um personenbezogene Daten oder andere für die Organisation wichtige Informationen im Sinne von Unternehmenswerten handelt.

ISO 27001 fordert, dass das verbleibende Risiko von einem Mitglied der Leitung der Organisation (Behördenleiter, Geschäftsführer) persönlich verant-

wortet werden muss; dies ist in einem handschriftlich unterschriebenen Dokument zu bestätigen.

Insbesondere bei personenbezogenen Daten mit hohem oder sehr hohem Schutzbedarf kann die automatisierte Verarbeitung der Daten aber auch unzulässig sein, wenn der Schutz der Daten in dem betreffenden Verfahren nicht sichergestellt werden kann.

Im Anhang A, der zum normativen Teil von ISO 27001 gehört, ist der Datenschutz unter der Ziffer A.15.1.4 *„Data protection and privacy of personal information“* enthalten, aber nicht weiter differenziert. Eine ISO 27001-Zertifizierung, auch eine genuine, ist also ohne Datenschutz nicht zu haben.

Der Datenschutzbaustein B 1.5 der Grundschutzkataloge mit seinen konkreten Listen und Erläuterungen datenschutzspezifischer Gefährdungslagen und Maßnahmenbündel (s. o. Ziff. 6.3.1.1) ist kein Pflichtbaustein für die Zertifizierung nach ISO 27001, auch nicht für die des BSI auf der Basis von IT-Grundschutz. Es steht aber selbstverständlich jeder Organisation frei, ihn nicht nur beim Aufbau ihres ISMS zu verwenden, sondern ihn auch zusätzlich in die ISO 27001-Zertifizierung mit einzubeziehen.

Beim Aufbau eines Datenschutzmanagementsystems sind Checklisten sinnvoll, an denen sich die für die Datenverarbeitung verantwortlichen Stellen sowie deren Auftragnehmer beim Aufbau eines Datenschutzmanagementsystems orientieren können, sowie Werkzeuge zur technischen Unterstützung des Datenschutzmanagement-Prozesses.

6.3.2
Datenschutzmanagementsysteme

6.3.2.1
Aufbau eines Datenschutzmanagementsystems

Hier stellt sich zunächst die Frage, ob ein Datenschutzmanagementsystem autonom aufgebaut oder in ein Informationssicherheitsmanagementsystem (ISMS) integriert werden sollte. Aus den bisherigen Ausführungen ergibt sich eine Reihe von Argumenten für die Integration des Datenschutzmanagementsystems in das ISMS:

– Datenschutz setzt den IT-Grundschutz voraus.
– Zumindest im Bereich der Protokollierung gibt es eine gemeinsame Gestaltungsaufgabe.
– Der Datenschutz ist in der Norm ISO 27001 enthalten (Anhang A, Ziffer A.15.1.4).

– Es gibt den Baustein B 1.5 Datenschutz in den Grundschutzkatalogen des BSI.

Umgekehrt müssten in ein autonomes Datenschutzmanagementsystem fast alle Anforderungen an die IT-Sicherheit mit aufgenommen werden.

Ein Datenschutzmanagementsystem sollte daher sinnvollerweise auf einem normierten bzw. standardisierten ISMS aufsetzen. Es bietet sich an, nach ISO 27001 zu verfahren und zusätzlich den Datenschutzbaustein der Grundschutzkataloge zu verwenden und verbindlich in die Zertifizierung mit einzubeziehen. Falls sich zukünftig wichtige zusätzliche Datenschutzthemen ergeben, die damit nicht abgedeckt sind, kann man sich an eine der deutschen Datenschutzkontrollinstanzen wenden, damit der Autor des Bausteins, der Arbeitskreis Technische und organisatorische Fragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, den Baustein ggf. entsprechend anpasst oder erweitert.

Die Vorteile einer Integration des Datenschutzmanagementsystems in das ISMS sind:

– Es gibt bereits einen internationalen Standard mit klaren Vorgaben.
– Es gibt zwei auf diesem Standard beruhende Zertifizierungsverfahren: ein internationales sowie ein weiter differenziertes nationales auf der Basis von IT-Grundschutz.
– Die Auditoren werden jeweils nach der Norm ISO 27006, also nach den gleichen Kriterien, akkreditiert.
– Der vorhandene Datenschutzbaustein kann bei Bedarf erweitert werden.
– ISO 27001 fordert eine Koordinierung der Informationssicherheit durch Repräsentanten von verschiedenen Teilen der Organisation mit relevanten Rollen und Funktionen. Es ist sinnvoll, hieran sowohl den IT-Sicherheitsbeauftragten als auch den betrieblichen bzw. behördlichen Datenschutzbeauftragten zu beteiligen. Die IT-Sicherheitsleitlinie für die Hessische Landesverwaltung schreibt genau das für die IT-Sicherheitsmanagementteams der Dienststellen vor. Dieses Gremium kann und sollte gleichzeitig die Koordination im Bereich des Datenschutzes übernehmen. Nur so wird die gestalterische Aufgabe aus Ziffer 6.3.1.1 gelöst und gleichzeitig Doppelarbeit vermieden.

Die am Markt befindlichen Versuche von Unternehmen, eigene Datenschutzmanagementsysteme zu definieren, reichen von einer unvollständigen Zusammenstellung der datenschutzrechtlichen Regelungen des BDSG bis hin zu einer weitgehenden Übernahme des Datenschutzbausteins der Grundschutzkataloge des BSI ergänzt durch Teile anderer Normen und Standards.

Aus meiner Sicht erscheint es nicht sinnvoll, weitere Datenschutzmanagementsysteme zu kreieren und damit von Nutzern in Wirtschaft und Verwaltung zusätzlich noch eine zeit- und kostenaufwändige Auswahl eines geeigneten proprietären Systems zu verlangen. Vielmehr ist es empfehlenswert, als Standard die Norm ISO 27001 zusammen mit dem Datenschutzbaustein zu nutzen.

6.3.2.2
Zertifizierung von Datenschutzmanagementsystemen

Eine Zertifizierung von Datenschutzmanagementsystemen sollte wie die von ISMS stets nach umfassenden, sinnvollen und objektiven Kriterien erfolgen und auf abweichende Definitionen üblicher Begriffe verzichten. Weder eine Zertifizierung anhand eines lückenhaften Systems noch eine „Auditierung mit Augenmaß“, wie sie am Markt derzeit bereits angeboten werden, erscheint daher zielführend. Organisationen können nur dann von einem Audit profitieren, wenn alle Fakten klar benannt werden, unabhängig davon, ob es sich um Stärken oder noch um Schwächen handelt. Letztere können dann im Verlaufe des Managementprozesses gezielt in Angriff genommen werden.

Unternehmen, die im Bereich Datenschutzmanagementsysteme ihre Dienste anbieten wollen, sollten sich vielmehr als Auditoren nach der Norm ISO 27006 akkreditieren lassen und darüber hinaus die erforderliche Fachkunde im Datenschutzrecht sowie seiner technischen und organisatorischen Umsetzung erwerben.

Eine Zertifizierung eines ISMS nach ISO 27001 und demzufolge auch die eines Datenschutzmanagementsystems gemäß dem hier vorgeschlagenen Verfahren setzt immer eine – ggf. erweiterte – Risikoanalyse voraus. Insbesondere die Dokumente *„Statement of Application“*, das einem Sicherheitskonzept entspricht, und der *„Risiko-Behandlungsplan“*, die im Rahmen der ISO 27001-Zertifizierung erstellt werden, sind zentrale Dokumente auch für die Prüfung durch Datenschutzbeauftragte bzw. Aufsichtsbehörden. Dies gilt selbst dann, wenn nicht auf der Basis IT-Grundschutz zertifiziert wird, und selbstverständlich auch, wenn der Datenschutzbaustein nicht in die Zertifizierung einbezogen wurde.

6.3.3
Grenzen und Missverständnisse

6.3.3.1
Datenschutzrechtliche Grenzen

In den Rechtsvorschriften zum Datenschutz sind unbestimmte Rechtsbegriffe enthalten, die der Auslegung bedürfen. Dazu gehören u. a. die Begriffe Angemessenheit und Erforderlichkeit.

Eine Zertifizierung in Bezug auf die Umsetzung des Datenschutzes und die Einführung eines Datenschutzmanagements wird bei unbestimmten Rechtsbegriffen auf dokumentierten rechtlichen Wertungen aufsetzen.

Es ist nicht Zweck oder Inhalt der Zertifizierung, die von der Daten verarbeitenden Stelle selbst oder von Beratern oder anderen von ihr beauftragten Dritten getroffenen Wertungen und Auslegungen im Einzelnen zu überprüfen. Die Auditoren legen sie ihrer Tätigkeit zu Grunde und setzen sie damit als richtig bzw. zutreffend voraus. Sie müssen aber über die erforderliche rechtliche und technische Fachkunde verfügen, um die Umsetzung der datenschutzrechtlichen Ziele beurteilen zu können. Und selbstverständlich müssen sie in der Lage sein, offenkundige Mängel zu erkennen und diese dann im Audit darstellen. Dazu gehört beispielsweise die Verarbeitung von personenbezogenen Daten mit hohem Schutzbedarf, insbesondere der „besonderen Arten“ nach § 3 Abs. 9 BDSG wie Religionszugehörigkeit, Gesundheit etc., wenn eine erweiterte Risikoanalyse fehlt oder die erforderlichen Maßnahmen nicht umgesetzt sind.

Behördlichen bzw. betrieblichen Datenschutzbeauftragten wie auch Datenschutzaufsichtsbehörden gegenüber entfalten die getroffenen Wertungen aber keinerlei Bindungswirkung. Ihre Aufgabe ist eine unabhängige Prüfung der vorgenommenen Wertungen und Auslegungen im Hinblick darauf, ob sie rechtlich in Ordnung sind. Die Zertifizierung kann hier Hilfestellung sein, weil sie die für die Datenverarbeitung verantwortliche Stelle zwingt, überhaupt Überlegungen hierzu anzustellen und die getroffenen Wertungen und Auslegungen zu dokumentieren, und so die Prüfung erleichtert.

§ 9a BDSG befasst sich mit dem Datenschutzaudit. Dort heißt es in Satz 2: „Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“ Dieses Gesetz gib es noch nicht. Demzufolge kann auch kein Datenschutzaudit auf dieser Basis durchgeführt werden. Dennoch gibt es Unternehmen, die Zertifikate „gemäß § 9a BDSG“ ausstellen. Solange

das Verfahren nach § 9a BDSG nicht geregelt ist, ist einen solche Zertifizierung unzulässig und irreführend.

6.3.3.2
Inhaltliche Grenzen

Ein Informationssicherheitsmanagementsystem nach ISO 27001 zertifiziert nicht den IT-Grundschutz selbst, insbesondere nicht auf der Ebene von Produkten und Anwendungsverfahren. Vielmehr geht es hier darum, im Sinne des Plan-Do-Check-Act-Verfahrens eine dauerhafte Aktualität von Unterlagen und ständige Verbesserungen des Prozesses zu erreichen. Dieser Management-Prozess erlaubt bzw. befähigt, die Anforderungen an die IT-Sicherheit umzusetzen. Gegenstand ist hier also nicht die Informationssicherheit selbst, sondern die ständige Überprüfung und Verbesserung derselben. Analoges gilt für ein Datenschutzmanagementsystem.

Für konkrete Produkte oder Verfahren, die beschafft werden sollen oder die beim Auftragnehmer eingesetzt werden, kann und sollte die Umsetzung der Anforderungen der IT-Sicherheit durch eine Zertifizierung nach den *„Common Criteria (CC)“*, den *„Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“*, nachgewiesen und so das erforderliche Vertrauen geschaffen werden.

Gleichwohl umfasst nach Aussagen des BSI eine Zertifizierung nach ISO 27001 auf der Basis IT-Grundschutz auch eine Zertifizierung der Umsetzung des IT-Grundschutzes. Obwohl hier die Grundschutzkataloge zugrunde gelegt werden, halte ich diese Aussage in mehrfacher Hinsicht für problematisch:

1. Die ISO 27001-Zertifizierung eines ISMS durch das BSI basiert auf einem Stichprobenverfahren, bei dem je Bausteingruppe nur ein Baustein zufällig ausgewählt und geprüft wird. Das bedeutet, dass viele Bausteine gar nicht in die Prüfung einbezogen werden.
2. In vielen Bereichen wird nur geprüft, ob erforderliche Unterlagen wie Passwortrichtlinien, IT-Sicherheitskonzept etc. vorhanden sind, ohne dass diese Unterlagen inhaltlich geprüft werden.
3. Die Ebene der Anwendungsverfahren wird nicht bzw. nicht im erforderlichen Umfang einbezogen.
4. Maßnahmen können häufig auf verschiedenen Ebenen des ISO-OSI-Modells umgesetzt werden, in vielen Fällen ist sogar eine bestimmte Kombination von Maßnahmen auf verschiedenen Ebenen erforderlich. Daher ist bei der Zertifizierung des IT-Grundschutzes die vollständige Einbeziehung aller Ebenen erforderlich, um sicherzustellen, dass das

Gesamtsystem wirklich die erforderliche Sicherheit gewährleistet. Dies ist aber offensichtlich nicht der Fall.

Bestenfalls ergibt sich bei diesem Vorgehen eine gewisse Wahrscheinlichkeit bzw. ein gewisser Anschein dafür, dass der IT-Grundschutz bezüglich der RZ- oder Netzwerkinfrastruktur umgesetzt ist. Das ist aber im Vergleich mit der Aussage des BSI eine starke Einschränkung.

Ein Beispiel soll das erläutern: Bei einem Rechenzentrum, das seine Dienste einschließlich Anwendungsverfahren vielen öffentlichen Stellen im Rahmen der Auftragsverarbeitung zur Verfügung stellt, musste ich bei einer Prüfung feststellen, dass in einigen Fällen Daten mit hohem Schutzbedarf weder auf der Anwendungs- noch auf der Netzwerk- bzw. Leitungsebene verschlüsselt übertragen wurden. Damit ist die erforderliche Vertraulichkeit nicht gegeben. Dieses RZ ist aber vom BSI nach ISO 27001 auf der Basis IT-Grundschutz zertifiziert. Bei der erforderlichen ebenenübergreifenden, erweiterten Risikoanalyse hätte das diesem Auftragnehmer und dem Auditor auffallen müssen.

Dieses Beispiel zeigt, dass weder Auftraggeber noch Auftragnehmer sich auf Zertifizierungen allein verlassen können. Vielmehr müssen sie sich der Aussagen und Grenzen der Zertifikate bewusst sein und die erforderlichen weiteren Schritte und Maßnahmen dem entsprechend festlegen.

6.3.3.3 Missverständnisse

In diesem Abschnitt sollen noch einige Missverständnisse ausgeräumt werden, mit denen ich im Rahmen meiner Tätigkeit immer wieder konfrontiert werde.

Die für die Datenverarbeitung verantwortliche Stelle ist verpflichtet, die ihr anvertrauten Daten zu schützen. Sie kann dazu ein Datenschutzmanagementsystem aufbauen, muss das aber nicht. Das Gleiche gilt für den Auftragnehmer, der nicht für die Datenverarbeitung verantwortliche Stelle ist. Er kann aber den verantwortlichen Stellen ihre Pflicht zur Auftragskontrolle mit einer Zertifizierung nach ISO 27001 erleichtern und bei potenziellen Auftraggebern Vertrauen schaffen in die Sicherheit seines RZ-Betriebes. Entsprechendes gilt für eine Zertifizierung nach den CC.

Jede Zertifizierung kann Aufwand an anderen Stellen einsparen und Vertrauen schaffen. Sie kostet aber auch Zeit und Geld. Deshalb sollte sie nur nach allgemeinen Normen und Standards erfolgen, um eine Vergleichbarkeit der Zertifikate und der mit ihnen getroffenen Aussagen und Wertungen

zu ermöglichen. Und sie sollte möglichst gut softwaretechnisch, organisatorisch und personell unterstützt werden, um den Gesamtaufwand in Grenzen zu halten. Der Begriff „Standard“ wird hier im Sinne der klaren Definition der British Standards (früher British Standards Institute) verstanden:

> *Ein Standard ist ein öffentlich zugängliches technisches Dokument, das unter Beteiligung aller interessierten Parteien entwickelt wird und deren Zustimmung findet. Der Standard beruht auf Ergebnissen aus Wissenschaft und Technik und zielt darauf ab, das Gemeinwohl zu fördern.*

6.3.4 Fazit

Beide Zertifizierungen, die nach ISO 27001 für Managementsysteme und die nach den CC für Produkte, können den Aufsichtsbehörden für den Datenschutz die Arbeit erleichtern ohne deren Kontrollen zu ersetzen oder vorwegzunehmen.

Datenschutz-Zertifikate greifen zu kurz, wenn sie einzelne Datenschutzanforderungen herausgreifen und zu einer positiven Gesamtbewertung kommen, ohne dass der IT-Grundschutz gewährleistet ist. Erst nach Umsetzung des IT-Grundschutzes und aller einschlägigen Datenschutzanforderungen können für besonders gute Lösungen in bestimmten Teilbereichen Pluspunkte vergeben werden.

Unternehmen, die im Bereich Auditierung und Zertifizierung von Datenschutzmanagementsystemen tätig werden wollen, sollten darauf verzichten, eigene Datenschutzmanagementsysteme zu entwerfen und sich stattdessen als Auditoren für ISO 27001 akkreditieren. Selbstverständlich erfordert dies zusätzlich Fachkunde sowohl im Datenschutzrecht selbst als auch im Bereich der Ziele des technischen und organisatorischen Datenschutzes sowie deren Umsetzung.

7. Bilanz

7.1
Novellierung des HSOG – Kennzeichenerkennung (38. Tätigkeitsbericht, Ziff. 4.2.1)

Mit der Novelle des HSOG Ende 2009 wurde u. a. eine neue Rechtsgrundlage zum Einsatz von Kennzeichenlesegeräten (AKLS) geschaffen, nachdem das Bundesverfassungsgericht die ursprüngliche Regelung des § 14 Abs. 5 HSOG im März 2008 für nichtig erklärt hatte.

Mit Beginn dieses Jahres kamen dann auch wieder AKLS zum Einsatz. Dies habe ich zum Anlass genommen, zu überprüfen, ob diese Geräte und die Einsatzpraxis mit den Vorgaben des Bundesverfassungsgerichts sowie der geänderten Rechtsgrundlage in Einklang stehen.

Es waren keine neuen Geräte beschafft worden. Im Betrieb wird das AKLS mit einem Laptop verbunden, auf dem sich der Fahndungsbestand befindet. Bei der Überprüfung musste ich feststellen, dass einige Nachbesserungen erforderlich waren.

Während des Betriebes des AKLS wurde auf dem angeschlossenen Laptop laufend die Liste der zehn letzten gelesenen Kennzeichen angezeigt. Parallel dazu bestand die Möglichkeit, sich das Bild des aktuell gelesenen Kennzeichens anzeigen zu lassen. Dieses Bild blieb so lange stehen, bis die Bildanzeige mit der Taste F5 aktualisiert wurde. Es stellte sich daher die Frage, wann genau die Löschung der Daten zu Fahrzeugen erfolgt, die keine Treffer sind.

Dies war zwar keine Veränderung des Systems zu dem im Jahr 2007 kontrollierten Einsatz an einer Autobahn. Damals wurde jedoch aufgrund des Verkehrsaufkommens die Liste der gelesenen Kennzeichen so schnell überschrieben, dass es gar nicht möglich war, diese am Bildschirm zu lesen. Durch die veränderten Rahmenbedingungen bei der Kontrolle an einer Straße im Stadtgebiet wurde jetzt deutlich, dass die Liste der gelesenen Kennzeichen teilweise nur sehr unregelmäßig überschrieben wurde. Je nach Einsatzort war es nicht ausgeschlossen, dass gelesene Kennzeichen auch mehrere Minuten in der Liste nachvollziehbar waren. Zumal sich die Anzeige des Fahrzeugbildes auf dem Bildschirm in diesem Zeitraum ggf. sogar noch verlängerte. Denn die Bilder wurden nicht automatisch verworfen, sondern nur durch einen Druck auf die Taste F5. Solange der Eintrag in der Liste oder das Bild am Bildschirm sichtbar waren, wären daher weitere Abfragen z. B. in POLAS durch die kontrollierenden Beamten möglich.

Dies war eine Behandlung von Nichttrefferfällen, die nicht mit den Vorgaben des Bundesverfassungsgerichts und auch nicht denen des § 14a HSOG im

Einklang steht. Das Bundesverfassungsgericht hatte in seiner Entscheidung vom 11. März 2008 ausgeführt, dass nur dann kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt, wenn nach unverzüglichem Abgleich und ohne die Möglichkeit weiterer Auswertungen, Nichttreffer sofort wieder gelöscht werden. Dazu muss für den Nichttrefferfall rechtlich und technisch abgesichert sein, dass sofort spurenlos gelöscht wird. Deshalb sieht § 14a Abs. 3 HSOG vor, dass die sog. Nichttrefferfälle sofort automatisiert zu löschen sind.

Die Software wurde daraufhin überarbeitet. In einem weiteren Termin konnten sich meine Mitarbeiter von der nunmehr den rechtlichen Anforderungen entsprechenden Ausgestaltung überzeugen. Gelesene Kennzeichen, die nicht im Fahndungsbestand enthalten sind, werden in der Benutzeroberfläche nicht mehr angezeigt. Um gleichzeitig die Überwachung der Funktionalität des Geräts sicherzustellen, erfolgt stattdessen eine Anzeige „Kennzeichen gelesen“. Dieser Anzeige sind zusätzlich die Qualität des Scanvorgangs (in Prozent), die Länderkennung des gelesenen Kennzeichens sowie ein Zeitstempel (Datum/Uhrzeit) angefügt.

7.2
Sicherheitspartnerschaft/Videoüberwachung (39. Tätigkeitsbericht, Ziff. 4.1.3)

Im letzten Jahr hatte ich gefordert, dass die Zusammenarbeit von kommunalen Ordnungsbehörden, Landes- und Bundespolizei bei der Videoüberwachung im Umfeld von Bahnhöfen klarer Zuständigkeitsregeln i. S. d. Hessischen Gesetzes für öffentliche Sicherheit und Ordnung und des Bundespolizeigesetzes bedürfe.

Insbesondere war hier zu berücksichtigen, dass für den Bereich der Bahnanlagen die Überwachungsbefugnis bei der Bundespolizei liegt (§ 3 BPolG), die in aller Regel aber nicht vor Ort und deshalb schon faktisch kaum in der Lage ist, Überwachungsmaßnahmen durchzuführen.

§ 3 Abs. 1 BPolG

Die Bundespolizei hat die Aufgabe, auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren, die
1. den Benutzern, den Anlagen oder dem Betrieb der Bahn drohen oder
2. beim Betrieb der Bahn entstehen oder von den Bahnanlagen ausgehen.

Im Laufe des Jahres ist es gelungen einen Weg zu finden, die ortsnahen Beteiligten mit der Überwachung von Bahnanlagen zu beauftragen, ohne in die Zuständigkeiten der Bundespolizei einzugreifen. Dies war möglich, da

für alle Beteiligten grundsätzlich eine gesetzliche Möglichkeit besteht, Videotechnik in diesem Kontext einzusetzen. Während für die Kommune und die Hessische Polizei sich dies aus § 14 Abs. 3 und 4 HSOG ergibt, sind die Einsatzvoraussetzungen für die Bahnpolizei in § 27 BPolG geregelt.

§ 27 BPolG

Die Bundespolizei kann selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einsetzen, um

1. *unerlaubte Grenzübertritte oder Gefahren für die Sicherheit an der Grenze oder*
2. *Gefahren für die in § 23 Abs. 1 Nr. 4 bezeichneten Objekte oder für dort befindliche Personen oder Sachen*

zu erkennen. In den Fällen des Satzes 1 Nr. 2 muss der Einsatz derartiger Geräte erkennbar sein. Werden auf diese Weise personenbezogene Daten aufgezeichnet, sind diese Aufzeichnungen in den Fällen des Satzes 1 Nr. 1 spätestens nach zwei Tagen und in den Fällen des Satzes 1 Nr. 2 spätestens nach 30 Tagen zu vernichten, soweit sie nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden.

Im Polizeirecht ist es zulässig, dass aufgrund entsprechender Vereinbarungen Polizeibehörden auf dem Zuständigkeitsgebiet einer anderen Polizeibehörde tätig werden. Eine entsprechende Vereinbarung wird es daher nun im Rahmen einer Sicherheitspartnerschaft für den Bereich des S-Bahnhofes geben. Gleichzeitig werden bestimmte Mitarbeiter des Ordnungsamtes als Hilfspolizeibeamte für die Bundespolizei eingesetzt.

Mit einer solchen Lösung kann nach meiner Einschätzung eine derartige Sicherheitspartnerschaft grundsätzlich eingegangen werden. Dies entbindet natürlich nicht von der Verpflichtung, vorab jeweils sorgfältig zu prüfen, ob die gesetzlichen Voraussetzungen zum Einsatz von Videotechnik für alle Beteiligten auf deren jeweils spezieller Rechtsgrundlage erfüllt sind.

7.3
Novellierung des Verfassungsschutzgesetzes (36. Tätigkeitsbericht, Ziff. 5.3.1.2)

Im 36. Tätigkeitsbericht (Ziff. 5.3.1) hatte ich über die Novellierung des Verfassungsschutzgesetzes im Jahr 2007 berichtet. Eines der Ziele war damals, die schon bestehenden Befugnisse zur akustischen und optischen Wohnraumüberwachung an die Vorgaben des Bundesverfassungsgerichts (Urteil vom 3. März 2004 – BVerfGE 109, 279) anzupassen. In den Gesetzestext aufgenommen wurde damals allein die Formulierung, dass die Behörde dafür Sorge zu tragen hat, dass „in keinem Fall in den Kernbereich privater Lebensgestaltung“ eingegriffen wird. Eine Konkretisierung erfolgte erst in

der Gesetzesbegründung. Ich hatte deshalb gefordert, die in der Gesetzesbegründung enthaltenen Vorgaben in eine Norm konkretisierende Verwaltungsvorschrift des HMDIS aufzunehmen. Eine derartige Dienstvorschrift für das Landesamt ist dieses Jahr endlich erarbeitet worden und im August in Kraft getreten. Danach ist für den Einsatz nachrichtendienstlicher Mittel (also nicht nur für die akustische und optische Wohnraumüberwachung) geregelt, dass der Einsatz dieser Mittel zu unterbleiben hat, wenn Erkenntnisse aus dem absolut geschützten Kernbereich erfasst werden. Wenn sich erst während des Einsatzes nachrichtendienstlicher Mittel Anhaltspunkte dafür ergeben, dass der Kernbereich betroffen ist, ist der Einsatz sofort zu unterbrechen. Er darf erst dann wieder fortgesetzt werden, wenn eine derartige Kernbereichsberührung nicht mehr zu befürchten ist. Des Weiteren dürfen Daten, die in den Kernbereich privater Lebensgestaltung fallen, nicht verwertet werden und sind unverzüglich zu löschen.

7.4
Hessisches Analyse- und Recherchesystem (HARIS) (38. Tätigkeitsbericht, Ziff. 4.3.1; 39. Tätigkeitsbericht, Ziff. 4.3.1)

Bei der Umsetzung des Hessischen Analyse- und Recherchesystems HARIS beim Hessischen Landesamt für Verfassungsschutz ergaben sich im Berichtsjahr aufgrund technischer und organisatorischer Probleme Verzögerungen. HARIS läuft weiterhin als Pilot mit Echtdaten. Geplant war, dass HARIS im Sommer 2011 in den Wirkbetrieb gehen sollte. Migriert wurden bis Ende 2010 alle Sachbereiche außer den Sicherheitsüberprüfungen. Die Anpassung der Software, die auch die verschiedenen Nachberichtspflichten bei den Sicherheitsüberprüfungen und Zuverlässigkeitsüberprüfungen organisieren soll, war Ende 2011 noch nicht abgeschlossen. Probleme gab es auch bei der Programmierung der Schnittstelle von HARIS zu dem neuen System NADIS WN. Dies hat zur Folge, dass HARIS frühestens Mitte 2012 in den Wirkbetrieb gehen kann und voraussichtlich Ende 2012 mit allen Funktionen einsatzfähig sein wird.

7.5
Ausbau des Nachrichtendienstlichen Informationssystem NADIS zu einem Wissens- und Informationsmanagementsystem (39. Tätigkeitsbericht, Ziff. 3.1)

Im 39. Tätigkeitsbericht (Ziff. 3.1) hatte ich über den Ausbau von NADIS zu einem Wissens- und Informationsmanagementsystem berichtet. Anders als geplant ist NADIS WN in seiner ersten Version (WN 1.0) im Herbst 2011 nicht

in Betrieb gegangen. Als neuer Termin wird jetzt das Frühjahr 2012 anvisiert. Die von mir im letzten Tätigkeitsbericht geschilderten Probleme sind noch nicht gelöst. Nach wie vor ist für einen umfangreichen Aufgabenbereich des Verfassungsschutzes aus rechtlichen Gründen nur ein Aktenhinweissystem und keine Textdatei möglich. Ein Entwurf für eine Änderung der gesetzlichen Grundlage liegt nicht vor. Es bestehen auch weiterhin Probleme bei der Aufnahme von Ursprungsdokumenten. Das HLfV beabsichtigt jedenfalls während der ersten Version von NADIS WN (NADIS WN 1.0) keine derartigen Dokumente einzustellen. Als problematisch hat sich auch die Schnittstelle von der Amtsdatei HARIS zu NADIS WN herausgestellt. Die Programmierung der Schnittstelle ist aufwändiger als geplant und führte zur Zeitverschiebung. Vorgesehen ist, dass die in der Amtsdatei HARIS gespeicherten Daten in NADIS WN eingestellt werden, u. a. um sie auch anderen Landesämtern für Verfassungsschutz und dem Bundesamtes für Verfassungsschutz zur Verfügung zu stellen.

7.6
Weiterhin in der Diskussion: Die Ausgestaltung der Zugriffe auf Krankenhausinformationssysteme (39. Tätigkeitsbericht, Ziff. 4.7.1)

In meinem 38. Tätigkeitsbericht (Ziff. 4.6.2.2.1) sowie dem 39. Tätigkeitsbericht (Ziff 4.7.1.2) habe ich über eine Prüfung der Zugriffsausgestaltung im Klinikum Kassel berichtet. Bei der Prüfung habe ich erhebliche Defizite bei der Ausgestaltung der Entscheidungsstrukturen, der Zugriffsberechtigungen und der Abläufe festgestellt. Eine Reihe von Defiziten wurden bereits während der Prüfung oder zeitnah, einige zu einem späteren Zeitpunkt beseitigt, die Umsetzung anderer Forderungen stand 2011 noch aus. Im April 2011 haben meine Mitarbeiter vor Ort eine erneute Prüfung zum aktuellen Sachstand der Zugriffsausgestaltung im Klinikum Kassel durchgeführt. Die neue Orientierungshilfe (s. Ziff. 3.8.3) wurde bei der Prüfung berücksichtigt. Nachfolgend werden die zentralen Prüfergebnisse, meine Forderungen sowie der Sachstand 2011 dargestellt.

7.6.1
Ausgestaltung der Benutzergruppen und Kontrollmöglichkeiten

Das Klinikum hatte meine Kritikpunkte aufgegriffen und für die ca. 2.500 Mitarbeiter die Anzahl der Benutzerprofile wesentlich reduziert.

Gegenstand von Diskussionen war bei der Prüfung insbesondere eine Benutzergruppe, die medizinische Daten von profilfremden Patienten nach

Eingabe einer Begründung sehen kann. Die auf diesem Weg erfolgten profilfremden Zugriffe wurden in einer gesonderten Tabelle protokolliert. Dies sollte sicherstellen, dass profilfremde Daten nur aufgerufen werden, wenn sie für die Aufgabenerfüllung der Mitarbeiter tatsächlich erforderlich sind. Grundsätzlich ist dies zu begrüßen. Es setzt allerdings voraus, dass die Gründe, die für den Zugriff angeklickt werden müssen, den tatsächlich im Alltag zu erfüllenden Aufgaben entsprechen und so formuliert sind, dass bei Durchsicht der Protokolle bereits eine angemessene Plausibilitätsprüfung durchgeführt werden kann. Die Prüfung ergab, dass beides zu diesem Zeitpunkt nicht der Fall war. Die zur Verfügung stehenden Gründe konnten zum einen nicht klar definiert und zum anderen auch nicht klar von einander abgegrenzt werden, zudem spiegelten sie z. T. nicht die Aufgaben der Mitarbeiter wieder.

Meine Forderung:
Die Verwendung des Begründungsfeldes ist anzupassen und organisatorisch zu regeln.

In der Zwischenzeit hat das Klinikum in Abstimmung mit dem ärztlichen Dienst vier Standardfälle zur Auswahl klar formuliert.

Ein weiterer Diskussionspunkt war die Frage, warum über die mit differenzierten Zugriffsrechten ausgestatteten Benutzergruppen hinaus die Einrichtung einer zusätzlichen Benutzergruppe mit umfassenden Sonderrechten und die Zuordnung zahlreicher Mitarbeiter zu dieser Benutzergruppe erforderlich war. Das Klinikum hat die Gründe für die Einrichtung dieser Benutzergruppe nach der Prüfung nachvollziehbar dargelegt und den Kreis der betreffenden Mitarbeiter wesentlich eingeschränkt.

7.6.2
Gemeinsame Patientenstammdatenhaltung von der Klinikum Kassel GmbH und der ZMV GmbH

Nach wie vor erfolgt bei jeder Aufnahme eines Patienten eine Prüfung, ob der Patient bereits angelegt ist; bei dieser Prüfung werden routinemäßig Stammdaten sowohl aller Patienten des Klinikums wie auch Stammdaten aller Patienten des ZMV angezeigt. Damit können Mitarbeiter des Klinikums die Daten von Patienten des ZMV sehen, die nicht im Klinikum behandelt werden und umgekehrt. Dies ist ein Verstoß gegen die ärztliche Schweigepflicht und die datenschutzrechtlichen Vorschriften.

Meine Forderung:
Die gemeinsame Patientenstammdatenhaltung von Klinikum und MVZ muss schnellstmöglich beseitigt werden.

Das Klinikum hat im Oktober mitgeteilt, dass es zum einen nach einer Alternative zum derzeit eingesetzten KIS sucht und zum anderen mit dem derzeitigen KIS-Hersteller mögliche kurzfristige Maßnahmen für eine datenschutzkonforme Lösung ermittelt.

7.6.3 Protokollierung

Mittlerweile werden im Klinikum alle lesenden Zugriffe protokolliert. Eine Protokollierung erfüllt allerdings nur ihren Zweck, wenn die Protokolle auch in effektiver Weise ausgewertet werden. In diesem Punkt wurde bei der Prüfung noch Handlungsbedarf festgestellt.

Meine Forderung:
Organisatorische Regelungen zum Einsatz der Protokollierung sind noch festzulegen, insbesondere zu den Fragen, wer die Auswertungen durchführt, in welchen Zeiträumen sie erfolgen, wie bei Auffälligkeiten zu verfahren ist und welche Verfahrensweisen dabei zu beachten sind.

Inzwischen hat das Klinikum ein eigenes Programm für die Protokollauswertungen weiterentwickelt, dem stellvertretenden Datenschutzbeauftragten des Klinikums eine organisatorische Anweisung zur Überprüfung fachübergreifender Zugriffe übermittelt und Rahmenbedingungen für die Verwendung der Protokolle festgelegt.

7.6.4 Benutzerverwaltung

Bei der Prüfung wurde festgestellt, dass der IT-Abteilung alle Benutzerkennwörter bekannt sind. Diese Verfahrensweise entspricht nicht den üblichen Standards und hebelt sämtliche Schutzmechanismen aus, die auf der Verwendung von Benutzerkennung und Passwort aufbauen.

Meine Forderung:
Es ist bei der Benutzerdefinition ein Standardpasswort festzulegen. Dieses ist dem Benutzer mitzuteilen und es ist sicherzustellen, dass dieser dieses Passwort sofort ändert. Das Passwort ist durch den Benutzer regelmäßig zu ändern.

Das Klinikum hat mir mitgeteilt, dass diesen Forderungen uneingeschränkt zugestimmt wird und die Forderungen so schnell wie möglich umgesetzt werden.

8. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

8.1
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Keine Vorratsspeicherung und Rasterung von Flugpassagierdaten!

Die EU-Kommission hat am 2. Februar 2011 einen neuen Entwurf für eine Richtlinie zur Nutzung von EU-Flugpassagierdaten zur Gefahrenabwehr und Strafverfolgung vorgestellt.

Zentraler Gegenstand des Entwurfs ist die systematische Erfassung der Daten aller Fluggäste, die EU-Außengrenzen überqueren. Diese Daten aus den Buchungssystemen der Fluggesellschaften sollen anlass- und verdachtsunabhängig an eine nationale Zentralstelle der Sicherheitsbehörden übermittelt und regelmäßig für fünf Jahre gespeichert werden. Ziel soll es sein, damit Personen ausfindig zu machen, die in Terrorismus oder schwere Kriminalität verwickelt sein könnten.

Auch der neue Entwurf bleibt konkrete Beweise dafür schuldig, dass die anlassfreie automatisierte Auswertung und Analyse von Flugpassagierdaten geeignet und erforderlich ist, um dieses Ziel zu fördern. Ein solches Zusammenspiel von Vorratsspeicherung und Rasterung von Passagierdaten ist weder mit der EU-Grundrechtecharta noch mit dem grundgesetzlich garantierten Recht auf informationelle Selbstbestimmung vereinbar. Dies gilt insbesondere im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts, das in seinem Urteil vom 2. März 2010 (1 BvR 256/08) zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten gemahnt hat: Zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört es, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Hierfür hat sich die Bundesrepublik auch auf europäischer und internationaler Ebene einzusetzen.

Ein solches System würde noch weiter reichende Eingriffe in die Bürgerrechte ermöglichen, wenn sogar Vorschläge zur Speicherung der Fluggastdaten bei Flügen innerhalb der Europäischen Union und von Daten der Bahn- und Schiffsreisenden Eingang in diese Richtlinie finden würden.

Dieser Entwurf verdeutlicht erneut, dass ein schlüssiges Gesamtkonzept auf europäischer Ebene zur Datenverarbeitung im Bereich der inneren Sicherheit fehlt, welches die Grundrechte der Betroffenen hinreichend gewährleistet.

Die Konferenz fordert daher die Bundesregierung und den Bundesrat auf, sich dafür einzusetzen, dass der Vorschlag der EU-Kommission für eine Richtlinie über die Verwendung von Passagierdaten nicht realisiert wird.

8.2
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten

Wollen Strafverfolgungsbehörden verschlüsselte Internetkommunikationsvorgänge (z. B. Internettelefonie oder E-Mails) überwachen und aufzeichnen, muss regelmäßig auf dem Endgerät des Betroffenen eine Software angebracht werden, die die Daten aus dem laufenden Kommunikationsvorgang vor ihrer Verschlüsselung erfasst und an die Behörde weiterleitet (sog. Quellen-Telekommunikationsüberwachung). Die hierbei anzuwendende Technik entspricht der der Online-Durchsuchung, die grundsätzlich auch Zugriffe auf gespeicherte Inhalte ermöglicht.

Telekommunikationsüberwachungsmaßnahmen durch Zugriffe auf Endgeräte müssen sich auf Daten aus laufenden Telekommunikationsvorgängen beschränken. Dies ist durch technische Vorkehrungen und rechtliche Vorgaben sicherzustellen. Nur so wird der Rechtsprechung des Bundesverfassungsgerichts entsprochen.

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

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, Rechtssicherheit – auch für die Strafverfolgungsbehörden – zu schaffen und die Zulässigkeit und die Voraussetzungen der Quellen-Telekommunikationsüberwachung unter strenger Beachtung der Vorgaben des Bundesverfassungsgerichts zu klären.

8.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt die Notwendigkeit, durch umfassende allgemein gültige Regelungen für den Datenschutz am Arbeitsplatz mehr Rechtssicherheit zu erreichen und bestehende Schutzlücken zu schließen. Dieser Ansatz erfordert klare gesetzliche Begrenzungen der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten. Die Bundesregierung und die Bundestagsfraktionen der SPD und von BÜNDNIS 90/DIE GRÜNEN haben hierzu Gesetzentwürfe vorgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Deutschen Bundestag, bei den Beratungen über Regelungen des Beschäftigtendatenschutzes insbesondere folgende notwendige Anforderungen sicherzustellen:

- Im Bewerbungsverfahren und im Beschäftigungsverhältnis
  - ist die Erforderlichkeit von Eignungstests und medizinischen Untersuchungen vor der Durchführung der jeweiligen Maßnahme zu dokumentieren,
  - sind Datenerhebungen nur zulässig, wenn und soweit diese Daten wegen der Art und der Ausübung der Tätigkeit oder der Bedingung ihrer Ausübung unabdingbar sind und entscheidende berufliche Anforderungen oder Hindernisse darstellen,
  - sind Eignungstests ausschließlich zulässig, wenn sie auf einer wissenschaftlichen Methode beruhen.
- Arbeitgeber müssen verpflichtet werden, Bewerber so früh wie möglich umfassend über die Datenerhebung aus allgemein zugänglichen Quellen (z. B. im Internet) und bei Dritten zu unterrichten.
- Zur Aufdeckung von Straftaten und ähnlich schwerwiegenden Pflichtverletzungen dürfen Beschäftigtendaten nur oberhalb normenklarer und verhältnismäßiger Einschreitschwellen erhoben und verwendet werden. Arbeitgeber dürfen dabei – insbesondere verdeckte – Überwachungsmaßnahmen nur ergreifen, wenn zu dokumentierende Tatsachen vorliegen. Mit Blick auf rechtsstaatliche Anforderungen ist die Grenze zwischen eigenverantwortlichen Recherchen des Arbeitgebers und der den Strafverfolgungsbehörden vorbehaltenen Aufgaben eindeutig zu bestimmen. Aus präventiven Gründen ist eine verdeckte Datenerhebung unzulässig.

- Insbesondere bezüglich der Durchführung von Screening-Verfahren sind klare materielle Kriterien – z. B. Prüfung der Verhältnismäßigkeit, Vorliegen von tatsächlichen Hinweisen auf Unregelmäßigkeiten – erforderlich. Zudem sollten Arbeitgeber verpflichtet sein, die näheren Umstände, die den Abgleich veranlassen, vorab zu dokumentieren.
- Die an verschiedenen Stellen im Gesetzentwurf der Bundesregierung vorgesehenen Regelungen zur Verhaltens- und Leistungskontrolle sind nach wie vor zu weitgehend. Der Gesetzgeber muss hier strenge Voraussetzungen vorgeben. Die Konferenz weist auf die gefestigte verfassungsrechtliche Rechtsprechung zum unzumutbaren Überwachungsdruck hin.
- Die Konferenz der Datenschutzbeauftragten fordert, die offene Videoüberwachung stärker zu begrenzen und insbesondere
  - zu verbieten, die z. B. bei der Qualitätskontrolle anfallenden Daten zur Verhaltens- und Leistungskontrolle zu nutzen.
  - für Bereiche zu untersagen, die nicht nur „überwiegend“, sondern auch der privaten Nutzung dienen.
- Das Petitionsrecht darf nicht beschränkt werden. Beschäftigte müssen sich jederzeit an die zuständige Datenschutzaufsichtsbehörde wenden können, ohne deswegen benachteiligt oder gemaßregelt zu werden.
- In gesetzliche Regelungen zum Beschäftigtendatenschutz sind darüber hinaus Bestimmungen aufzunehmen
  - zur Personalaktenführung – einschließlich der automatisierten Personalaktenführung,
  - zur privaten Nutzung von Telekommunikationsdiensten,
  - zum Thema Whistleblowing,
  - zum Bereich der Videoüberwachung im öffentlich zugänglichen Bereich, bei denen Beschäftigtendaten mit anfallen,
  - zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung,
  - zum Konzerndatenschutz unter Berücksichtigung des internationalen Datenverkehrs.

8.4
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011

Gravierende Defizite bei der Umsetzung des SWIFT-Abkommens – dringender Handlungsbedarf auf nationaler und europäischer Ebene

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder missbilligt, dass – wie eine Prüfung der Gemeinsamen Kontrollinstanz von Europol ergeben hat[3] – EU-Zahlungsdaten auf der Grundlage viel zu abstrakter Anfragen von US-Seite umfassend in die USA übermittelt wurden. Im Ergebnis wurden damit nicht einmal die im Abkommen festgelegten unzureichenden Datenschutzregeln beachtet. Das europäische Polizeiamt Europol hat jedem US-Ersuchen zugestimmt, obwohl aufgrund der Abstraktheit der schriftlichen Ersuchen mit nur mündlicher Begründung eine abkommenskonforme Erforderlichkeitsprüfung durch Europol nicht möglich war. Die angeforderten Daten wurden stets ohne Abstriche in die USA übermittelt. Diese Vorgehensweise ist mit dem SWIFT-Abkommen und der Europol darin zugewiesenen datenschutzrechtlichen Wächterfunktion nicht vereinbar.

Nach dem SWIFT-Abkommen muss Europol im Interesse der EU-Bürgerinnen und Bürger gewährleisten, dass die Beschränkungen und Verfahrensvorgaben des Abkommens strikt beachtet werden. Europol ist demnach verpflichtet, alle US-Ersuchen auf die Beachtung dieser Beschränkungen und damit auf die Erforderlichkeit der Datenübermittlung zu überprüfen. Ohne die Zustimmung von Europol darf SWIFT keine EU-Zahlungsdaten an die USA übermitteln.

Die jetzt festgestellten Mängel bestätigen die bereits im Vorfeld des Abkommens von der Konferenz geäußerte Befürchtung, dass Europol seine Kontrollaufgabe bei SWIFT nicht angemessen wahrnimmt. Offenkundig werden die Voraussetzungen, unter denen das Europäische Parlament dem SWIFT-Abkommen zugestimmt hat, nicht eingehalten. Inakzeptabel ist auch, dass die festgestellten Details von Europol pauschal als geheim klassifiziert wurden und dem Europäischen Parlament nicht mitgeteilt werden sollen. Auch die Öffentlichkeit hat ein Recht darauf zu erfahren, in welchem Umfang Daten aufgrund des Abkommens in die USA übermittelt wurden.

Die Konferenz fordert die politisch Verantwortlichen auf europäischer und nationaler Ebene auf, die Mängel umgehend zu beseitigen. Das Abkommen

[1] Der von der Gemeinsamen Kontrollinstanz von Europol vor wenigen Tagen veröffentlichte öffentliche Teil des Kontrollberichts zur Umsetzung des SWIFT-Abkommens ist auf der Homepage der GKI (http://europoljsb.consilium.europa.eu/about.aspx) abrufbar.

und seine Umsetzungspraxis gehören dringend auf den Prüfstand. Ein transparentes Verfahren und die Beteiligung der Öffentlichkeit sind unabdingbar. Die gravierenden Mängel erfordern zudem einen sofortigen Stopp der Entwicklung eines vergleichbaren EU-Systems.

8.5
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juli 2011

Funkzellenabfrage muss eingeschränkt werden!

Die Strafverfolgungsbehörden in Dresden haben mit einer sog. Funkzellenabfrage anlässlich von Versammlungen und dagegen gerichteter Demonstrationen am 19. Februar 2011 Hunderttausende von Verkehrsdaten von Mobilfunkverbindungen erhoben, darunter die Rufnummern von Anrufern und Angerufenen, die Uhrzeit sowie Angaben zur Funkzelle, in der eine Mobilfunkaktivität stattfand. Dadurch sind zehntausende Versammlungsteilnehmerinnen und Versammlungsteilnehmer, darunter Abgeordnete von Landtagen und des Deutschen Bundestages, Rechtsanwältinnen und Rechtsanwälte, sowie Journalistinnen und Journalisten in Ausübung ihrer Tätigkeit, aber auch Anwohnerinnen und Anwohner der dicht besiedelten Dresdener Innenstadt, in ihrer Bewegung und ihrem Kommunikationsverhalten erfasst worden. Dieser Vorfall verdeutlicht die Schwäche der gesetzlichen Regelung.

Rechtsgrundlage der nichtindividualisierten Funkzellenabfrage ist bisher § 100g Abs. 2 S. 2 StPO, wonach im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation ausreichend sein soll, um Verkehrsdaten bei den Telekommunikationsdiensteanbietern erheben zu dürfen. Diese Aussage wird mit einer allgemeinen Subsidiaritätsklausel verknüpft. Diese 2001 in die Strafprozessordnung eingefügte Regelung ist unzureichend, da sie weder hinreichend bestimmt ist noch den heutigen technischen Gegebenheiten entspricht. Aktuelle Geräte erzeugen durch ihren Datenverkehr ohne aktives Zutun des Besitzers eine Vielzahl von Verkehrsdaten, die später in einer Funkzellenabfrage erhoben werden können.

Die Funkzellenabfrage ist ein verdeckter Eingriff in das Fernmeldegeheimnis (Art. 10 GG). Sie richtet sich unterschiedslos gegen alle in einer Funkzelle anwesenden Mobilfunkgerätebesitzer, nicht nur – wie etwa eine Telekommunikationsüberwachung nach § 100a StPO – gegen bestimmte einzelne Tatverdächtige. Sie offenbart Art und Umstände der Kommunikation von u. U. Zehntausenden von Menschen, die selbst keinen Anlass für einen staatlichen Eingriff gegeben haben. Sie schafft damit des Weiteren die Mög-

lichkeit, diese Personen rechtswidrig wegen Nicht-Anlasstaten, etwa Verstößen gegen das Versammlungsgesetz, zu verfolgen. Sie ist bezogen auf einzelne Personen ein Instrument der Verdachtsgenerierung. Die Strafprozessordnung regelt nicht näher, wie die Behörden mit den erhobenen Daten umzugehen haben, insbesondere nicht, über welche Zeiträume, zu welchen Personen und in welchen anderen Zusammenhängen die erhobenen Daten polizeilich weiter verwendet werden dürfen.

Das Bundesverfassungsgericht hat stets betont, dass die Erhebung von Verkehrsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulässt. Verkehrsdaten können das soziale Netz des Betroffenen widerspiegeln; allein aus ihnen kann die Verbindung zu Parteien, Gewerkschaften oder Bürgerinitiativen deutlich werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Bundesgesetzgeber auf, den Anwendungsbereich für eine nichtindividualisierte Funkzellenabfrage einzuschränken, dem Grundsatz der Verhältnismäßigkeit zu stärkerer Beachtung in der Praxis zu verhelfen, das Erforderlichkeitsprinzip zu stärken (etwa durch die Pflicht zur unverzüglichen Reduzierung der erhobenen Daten auf das zur Strafverfolgung oder gerichtlichen Auseinandersetzung Erforderliche) sowie die Löschungsvorschrift des § 101 Abs. 8 StPO zu präzisieren.

8.6
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011

Antiterrorgesetze zehn Jahre nach 9/11 – Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was

mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BTDrucks. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze – gerade in ihrem Zusammenwirken – durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

8.7
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutzkultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

8.8
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise

webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten *(privacy by design)* und dementsprechende Voreinstellungen wählen *(privacy by default)*. Internetnutzende sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.
- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.
- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.
- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.
- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-

Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.
- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).
- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.
- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.
- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ *whois* aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

8.9
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011

Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (LTDrucks. 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Daten-

schutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen kann. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

8.10
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook®, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social Plugins beispielsweise von Facebook®, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir“-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook® mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook® als auch Google+® verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BTDrucks. 17/6765) als einen Schritt in die richtige Richtung.

8.11
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BTDrucks. 17/6804) sieht vor, über bereits bestehende – allerdings nicht umgesetzte – gesetzliche Verpflichtungen hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

9. Gleichlautende Entschließungen der Datenschutzbeauftragten des Bundes und der Länder und Beschlüsse des Düsseldorfer Kreises

9.1
Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wie auch der Düsseldorfer Kreis haben auf die Notwendigkeit einer datenschutzkonformen Gestaltung und Nutzung von Informationstechnik in Krankenhäusern hingewiesen. Die Konferenz hat bereits im Oktober 2009 auf die Problematik aufmerksam gemacht und auch der Düsseldorfer Kreis erläutert zu der Thematik, dass Krankenhausinformationssysteme heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden sind. Ein Abruf der darin elektronisch gespeicherten Patientendaten sei jederzeit, ortsungebunden und sekundenschnell möglich und biete damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stünden allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, seien groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegten dies. Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern und erklären gemeinsam mit den Datenschutzbeauftragten von Bund und Ländern:

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder (eine Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales“ und „Technik“ der Konferenz) unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Krankenhäusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Auch für die Datenschutzbehörden im öffentlichen Bereich wird das Dokument als Maßstab bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 16./17. März und die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben in ihrer Sitzung am 4./5. März die Orientierungshilfe zustimmend zur Kenntnis genommen.

9.2
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 4./5. Mai 2011

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.
3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)

- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KVSafeNet eingehalten werden.

9.3
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 28./29. September 2011

Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,
- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[1] der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

In ihrer Sitzung am 22./23. November 2011 sind die Mitglieder des Düsseldorfer Kreises einstimmig der durch die Datenschutzkonferenz am 28./29. September 2011 gefassten Entschließung und der Orientierungshilfe „Cloud-Computing“ beigetreten.

[1] http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf

10. Beschlüsse des Düsseldorfer Kreises

10.1
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011

Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend – Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotenzial für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

– Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
– Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.
– Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

10.2
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 4./5. Mai 2011

Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“.

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

– Transparenz bezüglich der Preisgabe personenbezogener Daten: In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen

durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten: Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.
- Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung: Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.
- Anonyme und pseudonyme Nutzungsmöglichkeiten: Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risksopportunities-and-recommendations-for-users/at_download/fullReport).

10.3
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22./23. November 2011

Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern – und gegebenenfalls Daten Dritter – zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt.

Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.
- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.
- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

10.4
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22./23. November 2011

Anonymes und pseudonymes elektronisches Bezahlen von Internetangeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote – insbesondere Informationsdienste und Medieninhalte – nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BTDrucks. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment“) zu erhalten.

10.5
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. Dezember 2011

Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

– Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.

– Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.
– Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.
– Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten – soweit keine Einwilligung vorliegt – ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.
– Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.
– Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.
– Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.
– Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechts-

wirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

11. Materialien

11.1
Orientierungshilfe – Cloud Computing

der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

In der Arbeitsgruppe haben mitgewirkt:

Jens Budszus (Die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht Brandenburg)

Hanns-Wilhelm Heibey (Berliner Beauftragter für Datenschutz und Informationsfreiheit)

Renate Hillenbrand-Beck (Der Hessische Datenschutzbeauftragte)

Dr. Sven Polenz (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)

Marco Seifert (Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen)

Maren Thiermann (Der Hessische Datenschutzbeauftragte)

Inhaltsübersicht

0 Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich bereits seit längerer Zeit mit der Thematik des Cloud Computing. Da das Thema weiter an Aktualität gewonnen hat, wurde von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vorliegende Orientierungshilfe erarbeitet. Die Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern.

1 Einführung

1.1
Nutzen

„Cloud Computing“ steht für „Datenverarbeitung in der Wolke“ und beschreibt eine über Netze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung ausgelagert wird.[1] Teilweise wird von Cloud Computing auch dann gesprochen, wenn eine oder mehrere IT-Dienstleistungen (Infrastruktur, Plattformen, Anwendungssoftware) aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Anwendung abrechenbar über ein Netz bereitgestellt werden.[2]

[1] Weichert, Cloud Computing und Datenschutz, DuD 2010, 679. Vgl. auch Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, Meinungsspiegel: Was ist Cloud-Computing?, S. 147 ff.
[2] Alex D. Essoh (BSI): Cloud Computing und Sicherheit – Geht denn das?, 2009, www.bsi.bund.de/cln_174/ContentBSI/Aktuelles/Veranstaltungen/gstag/gstag_091119.html.

Cloud Computing kann auch als eine Form der bedarfsgerechten und flexiblen Anwendung von IT-Dienstleistungen verstanden werden, indem diese in Echtzeit als Service über das Internet bereitgestellt werden und danach eine Abrechnung erfolgt. Damit ermöglicht Cloud Computing eine Umverteilung von Investitions- und Betriebsaufwand. Die IT-Dienstleistungen können sich wiederum auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb sowie auf die Basisinfrastruktur beziehen. Dabei hat sich eine Einteilung in die drei Cloud-Services bzw. Organisationsformen „Software as a Service“, „Platform as a Service“ und „Infrastructure as a Service“ weitgehend durchgesetzt. Weiterhin wird zwischen „Public-, Private-, Hybrid-und Community-Clouds“ differenziert.[3]

Die Entstehung jener Form der Datenverarbeitung ist eng verbunden mit der enormen Steigerung der Rechenleistung, der flächendeckenden Verfügbarkeit höherer Bandbreiten für die Datenübertragung und der einfachen Einsetzbarkeit von Virtualisierungstechnologien. Als Synthese von IT-und Telekommunikations-Leistungen führt Cloud Computing dazu, dass – einfach dargestellt – jegliche Leistung als Service erhältlich wird. Cloud Computing repräsentiert somit den Gedanken von „Services aus dem Netz“, vergleichbar mit „Strom aus der Steckdose“. Cloud Computing lässt sich damit auch als eine dynamisch allokierbare Infrastruktur verstehen, in der Kapazitäten und Services nach Bedarf bezogen werden können und die Grundlage dieser Struktur in der Virtualisierung von Hardware, des Speichers, des Netzwerks und der Software besteht.[4]

Für die Anwendung von Cloud-Services sprechen vor allem wirtschaftliche Aspekte:

- Flexibilität bei der Buchung, Nutzung und Stilllegung von Rechenkapazitäten je nach aktuellem und ggf. auch kurzfristigem Bedarf (Skalierbarkeit)
- Einfacher Erwerb, verbrauchsabhängige Bezahlung
- Einsparpotenzial in den Bereichen Anschaffung, Betrieb und Wartung der IT-Systeme
- Ubiquitäre Verfügbarkeit von Geschäftsanwendungen unabhängig von geographischen Standorten.

[3] Vgl. BITKOM-Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, www.bitkom.org/de/themen/36129_61111.aspx.
[4] So Ulrich Roderer: Cloud Computing, SaaS, PaaS und IaaS verändert die Geschäftsmodelle der Dienstleister, 2010, www.searchdatacenter.de/themenbereiche/cloud/infrastruktur/articles/258317/.

1.2
Datenschutzrechtliche Schwerpunkte

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen von Cloud-Services sind alle datenschutzrechtlichen Bestimmungen einzuhalten.

Personenbezogen sind nur Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Ein verfassungsrechtlicher Schutz personenbezogener Daten besteht zudem durch das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[5] Die folgenden Erörterungen beziehen sich nur auf das für die nichtöffentlichen Stellen und die Bundesverwaltung geltende BDSG. Soweit die Anwendung von Cloud-Services auch für öffentliche Stellen an Bedeutung gewinnt, müssen diese die entsprechenden Regelungen in den Landesdatenschutzgesetzen einhalten. Teilweise entsprechen die Vorschriften der Landesdatenschutzgesetze im Wesentlichen den Vorschriften des BDSG, teilweise können aber auch erhebliche Unterschiede bestehen. Es ist daher eine sorgfältige Prüfung geboten.[6] Ebenso müssen spezielle Vorschriften beachtet werden, wie beispielsweise § 80 SGB X, der für die Auftragsdatenverarbeitung im Sozialbereich gilt. Für das Cloud Computing ergeben sich dabei sowohl aus Sicht des Datenschutzes als auch der Datensicherheit folgende Besonderheiten:

- Vermeintlich als anonymisiert angesehene Daten (vgl. § 3 Abs. 6 BDSG) können durch ihre Verarbeitung in der Cloud reidentifizierbar werden, weil verschiedene Beteiligte über Zusatzwissen verfügen, mit dem eine Reidentifizierung möglich ist.[7] Für die verantwortliche Stelle (§ 3 Abs. 7 BDSG) muss daher deutlich werden, in welchem Rahmen Datenschutzbestimmungen einzuhalten sind.
- Bei der Anwendung von Cloud-Services und der Bereitstellung von IT-Dienstleistungen werden regelmäßig mehrere Beteiligte tätig. Hier ist von Bedeutung, wie deren Beziehungen zueinander datenschutzrechtlich zu bewerten sind und wie vor allem die verantwortliche Stelle ihren Verpflichtungen nachkommt.
- Die verantwortliche Stelle hat die Rechtmäßigkeit der gesamten Datenverarbeitung zu gewährleisten, insbesondere muss sie ihren Löschpflichten nachkommen (§ 35 Abs. 2 BDSG), unrichtige Daten berichtigen (§ 35 Abs. 1 BDSG), für eine Sperrung von Daten sorgen (§ 35 Abs. 3

[5] BVerfG, Urteil v. 27.02.2008, 1 BvR 370/07.
[6] Siehe hierzu auch Endnote 26.
[7] Weichert, Cloud Computing und Datenschutz, DuD 2010, 679, 681.

BDSG) und dem Betroffenen (§ 3 Abs. 1 BDSG) u. a. Auskünfte über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, erteilen (§ 34 Abs. 1 BDSG). Zur Erfüllung der entsprechenden gesetzlichen Bestimmungen muss die verantwortliche Stelle besondere Vorkehrungen treffen.

- Zu untersuchen ist die Zulässigkeit grenzüberschreitender Datenverarbeitungen. Bei Clouds, die international verteilt sind und sich auch über Staaten außerhalb des EWR erstrecken, ist eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in Drittstaaten erforderlich.
- Aus technisch-organisatorischer Sicht müssen vor allem besondere Vorkehrungen für die ordnungsgemäße Löschung und Trennung von Daten sowie für die Sicherstellung von Transparenz, Integrität und Revisionsfähigkeit der Datenverarbeitung getroffen werden.

Bei Nichteinhaltung der Datenschutzbestimmungen drohen der verantwortlichen Stelle haftungsrechtliche Konsequenzen, indem diese gegenüber den Betroffenen zum Schadensersatz verpflichtet ist, Bußgelder verhängt oder Anordnungen (§ 38 Abs. 5 BDSG) verfügt werden können. Weiterhin entstehen bei unrechtmäßiger Kenntniserlangung von Daten gegenüber der zuständigen Aufsichtsbehörde und den Betroffenen Informationspflichten (§ 42a BDSG).

2 Begriffe

In der Praxis besteht keine einheitliche Terminologie der Begriffe. Die Definitionen haben sich an den Ausführungen des BSI und des Fraunhofer Institutes für Offene Kommunikationssysteme orientiert und werden der Bewertung zugrunde gelegt.

2.1
Cloud-Anwender

Cloud-Anwender ist jede natürliche oder juristische Person, die von Betroffenen personenbezogene Daten erhebt, verarbeitet oder nutzt und hierfür von anderen Stellen IT-Dienstleistungen für Cloud-Services in Anspruch nimmt.

2.2
Cloud-Anbieter

Cloud-Anbieter ist jede natürliche oder juristische Person, die einem Cloud Anwender IT-Dienstleistungen für Cloud-Services bereitstellt. Fehlen dem

Cloud-Anbieter hierfür die Ressourcen, so kann dieser zur Erfüllung seiner Verpflichtungen gegenüber dem Cloud-Anwender u. U. weitere Unter-Anbieter einbeziehen.

2.3
Public Cloud

IT-Dienstleistungen für Public Clouds werden am freien Markt und nicht innerhalb einer Institution oder im internen Unternehmensbereich einer verantwortlichen Stelle angeboten. Sie können folglich von einer beliebigen Zahl von Cloud-Anwendern in Anspruch genommen werden.[8]

2.4
Private Cloud

IT-Dienstleistungen werden hierbei innerhalb einer Institution oder im internen Unternehmensbereich einer verantwortlichen Stelle angeboten,[9] sodass der Cloud-Anwender und der Cloud-Anbieter (oder mehrere Cloud-Anbieter) dem Bereich dieser verantwortlichen Stelle zuzuordnen sind.[10]

2.5
Community Cloud

In einer Community Cloud schließen sich zwei oder mehrere Cloud-Anbieter aus Private Clouds zusammen, um für einen definierten Kundenkreis IT-Dienstleistungen für Cloud-Services zu erbringen.[11]

2.6
Hybrid Cloud

Bei Hybrid Clouds werden Public-, Private-und/oder Community Clouds miteinander kombiniert. Dieses Modell kann im Rahmen der Erhöhung der Verfügbarkeit oder zur effizienten Lastverteilung zum Einsatz kommen.

---

[8] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 22.
[9] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 20.
[10] Eine andere gängige Definition der Private Cloud ist die Bereitstellung von Cloud-Infrastruktur für nur einen einzigen Kunden durch einen externen Anbieter. Dies hat andere rechtliche und vertragliche Implikationen als die hier definierte Private Cloud.
[11] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 21.

2.7
Infrastructure as a Service (IaaS)

Cloud-Anwender erhalten Zugriff auf üblicherweise virtualisierte Komponenten zur Datenverarbeitung, zum Datentransport und zur Datenspeicherung. Sie können nahezu beliebige Anwendungsprogramme und Betriebssysteme einsetzen

2.8
Platform as a Service (PaaS)

Platform as a Service ermöglicht dem Cloud-Anwender, auf der vom Cloud-Anbieter angebotenen Infrastruktur eigene Programme zu entwickeln und auszuführen. Der Cloud-Anbieter macht hierbei Vorgaben zu den zu verwendenden Programmiersprachen und Schnittstellen zu Datenspeichern, Netzwerken und Datenverarbeitungssystemen. Wie bei der Dienstleistung Software as a Service auch, hat der Cloud-Anwender keine Möglichkeit, auf die zur Bereitstellung des Dienstes genutzte Infrastruktur administrativ oder kontrollierend zuzugreifen. Die Kontrollmöglichkeiten beschränken sich auf die selbst eingebrachten Programme und Daten.

2.9
Software as a Service (SaaS)

Der Zugriff des Cloud-Anwenders auf die vom Cloud-Anbieter bereit gestellten Anwendungen erfolgt üblicherweise über einen Web-Browser, kann aber auch mit speziellen Programmen erfolgen, die hauptsächlich über Anzeigefunktionen verfügen („Thin-Clients“). Software as a Service wird aufbauend auf Plattform-oder Infrastruktur-orientierten Cloud-Angeboten betrieben. Die bereitgestellten Anwendungen können allenfalls in geringem Umfang auf spezielle Anforderungen der Cloud-Anwender angepasst werden. Auf die für das Bereitstellen der Anwendung genutzten Dienste und Systeme haben die Cloud-Anwender regelmäßig keinen direkten administrativen, operativen oder kontrollierenden Zugriff.

3 Datenschutzrechtliche Aspekte

3.1
Verantwortlichkeit des Cloud-Anwenders

Das europäische und deutsche Datenschutzrecht knüpft die rechtliche Verantwortlichkeit für die Datenverarbeitung personenbezogener Daten an die inhaltliche Verantwortlichkeit über die Entscheidung des Umgangs mit den

Daten. Danach ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt und allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, § 3 Abs. 7 BDSG, Art. 2 Buchst. d) 4 Richtlinie 95/46/EG. Der Cloud-Anwender ist verantwortliche Stelle in diesem Sinne. Ein Cloud-Anbieter kann jedoch dann ausnahmsweise verantwortliche Stelle sein, wenn er selbst Dienstleistungen anbietet.[12]

Nimmt der Cloud-Anwender von einem Cloud-Anbieter IT-Dienstleistungen für Cloud-Services in Anspruch, so wird Letzterer als Auftragnehmer nach § 11 Abs. 2 BDSG tätig. Der Cloud-Anwender bleibt hingegen nach § 11 Abs. 1 BDSG für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich. Weiterhin muss der Cloud-Anwender einen schriftlichen Auftrag an den Cloud-Anbieter erteilen und dabei die inhaltlichen Anforderungen nach § 11 Abs. 2 BDSG erfüllen. Hilfreich kann hierfür beispielsweise die Mustervereinbarung zur Auftragsdatenverarbeitung des Hessischen Datenschutzbeauftragten in der Fassung des vom Regierungspräsidiums Darmstadt entwickelten Musters sein.[13]

Vertraglich festzulegen sind etwa die Berichtigung, Löschung und Sperrung von Daten. Die praktische Umsetzung dieser Verpflichtung kann durch technische Maßnahmen erfolgen (Kapitel 4.). Weiterhin ist z. B. nach § 11 Abs. 2 Nr. 6 BDSG zu regeln, ob eine Berechtigung zur Begründung von Unterauftragsverhältnissen besteht. Cloud-Anbieter werden zur Erbringung der IT-Dienstleistungen oft Unter-Anbieter einbeziehen, wobei auch für dieses Verhältnis die Regeln der Auftragsdatenverarbeitung zu erfüllen sind. Die Einbeziehung von Unter-Anbietern kann für den Cloud-Anwender intransparent sein, da deren Inanspruchnahme auch nur für einen kurzzeitig gestiegenen Bedarf an Rechenleistung in Betracht kommt und nicht deutlich wird, wessen Kapazitäten genutzt wurden. Der Cloud-Anbieter muss daher vertraglich verpflichtet werden, sämtliche Unter-Anbieter abschließend gegenüber dem Cloud-Anwender zu benennen und die für § 11 Abs. 2 BDSG relevanten Inhalte[14] offen zu legen. Der Unter-Anbieter ist zu verpflichten, die Weisungen des Auftragnehmers zu beachten.

Weiterhin besteht das Risiko eines auftragswidrigen Umgangs mit personenbezogenen Daten durch den Cloud-Anbieter, indem dieser z. B. Weisungen des Cloud-Anwenders missachtet und eine Verarbeitung und Nut-

[12] vgl. Art. 29-Datenschutzgruppe, WP 179, S. 27.
[13] http://www.datenschutz.hessen.de/mustervereinbarung_auftrag.htm
[14] Offenzulegen sind auch Vereinbarungen zwischen dem Auftragnehmer und Unterauftragnehmern, vgl. Klausel 5j des Controller-Processor-Standardvertrages, http://ec.europa.eu/justice/data-protection/document/internationaltransfers/transfer/index_en.htm#h2-5.

zung für eigene Geschäftszwecke vornimmt. Dem kann durch die Aufnahme einer Vertragsstrafenregelung entgegengewirkt werden. Weitere organisatorische sowie technische Gegenmaßnahmen werden unter 4. beschrieben.

3.2
Kontrolle der Cloud-Anbieter

Der Cloud-Anwender hat sich als Auftraggeber nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Dem Cloud-Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Cloud-Anbieters verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte Sicherheitsstandards eingehalten werden.[15] Die Lösung kann darin bestehen, dass der Cloud-Anbieter sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der Datensicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft.[16] Das Vorliegen von Zertifikaten entbindet den Cloud-Anwender nicht von seinen Kontrollpflichten nach § 11 Abs. 2 Satz 4 BDSG.

Besteht eine Erlaubnis zur Beauftragung von Unter-Anbietern, so müssen im Rahmen der Unterbeauftragung die Vorgaben des Vertrags zwischen Cloud-Anwender und Cloud-Anbieter berücksichtigt werden. Der Cloud-Anbieter muss in diesem Fall vor Beginn der Datenverarbeitung im Rahmen der Unterbeauftragung eine Kontrolle nach § 11 Abs. 2 Satz 4 BDSG vornehmen. Hierfür muss dann derselbe Kontrollmaßstab gelten wie im Verhältnis zwischen Cloud-Anwender und Cloud-Anbieter. Dabei ist zu fordern, dass der Cloud-Anwender die Begründung von Unteraufträgen davon abhängig macht, dass der Cloud-Anbieter entsprechende Vereinbarungen mit dem Unter-Anbieter trifft. Weiterhin sollte der Cloud-Anbieter gegenüber dem Cloud-Anwender vertraglich verpflichtet sein, auf Verlangen vorhandene Nachweise zu Zertifizierungen bzw. Datenschutz-Gütesiegeln der Unter-Anbieter vorzulegen.

[15] Wedde, in: Däubler/Klebe/Wedde/Weichert, Kommentar zum BDSG, 3. Aufl. 2010, § 11 Rndr. 55.

[16] Vgl. z. B. Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/guetesiegel/index.htm; Europäisches Datenschutz-Gütesiegel beim ULD, https://www.datenschutzzentrum.de/europrise/; Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/cln_174/DE/Themen/ZertifizierungundAnerkennung/ zertifizierungundanerkennung_node.html;jsessionid=19D1C64BFD37C3547FF0724D1D973F5A.

3.3
Betroffenenrechte

Der Cloud-Anwender bleibt als Auftraggeber nach § 11 Abs. 1 BDSG zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet, wobei ihm auch die Verpflichtung obliegt, personenbezogene Daten nach den §§ 34, 35 BDSG zu berichtigen, zu löschen, zu sperren und auf Verlangen des Betroffenen Auskünfte vor allem zu den zu seiner Person gespeicherten Daten und zur Herkunft der Daten zu erteilen. Da der Cloud-Anwender nur einen sehr eingeschränkten administrativen, operativen und kontrollierenden Zugriff auf die Infrastruktur des Cloud Computing hat, sollte er gegenüber dem Cloud-Anbieter vertragsstrafenbewehrte Weisungsrechte festlegen, die eine Erfüllung der Betroffenenrechte gewährleisten und diesem zusätzlich die Verpflichtung auferlegen, gegenüber Unter-Anbietern dieselben Rechte einzuräumen. Weiterhin können zur Durchsetzung der Betroffenenrechte technische Maßnahmen ergriffen werden (Kapitel 4).

3.4
Grenzüberschreitender Datenverkehr

Da die Cloud nicht an geographische Grenzen gebunden und darin stattfindende Datenverarbeitung gerade nicht ortsgebunden ist, muss für eine datenschutzrechtliche Betrachtung insbesondere deutlich werden, wo die Cloud-Anbieter und Unter-Anbieter tätig werden. Der Cloud-Anwender wird aber oft nicht wissen, an welchem „Ort“ im jeweiligen Augenblick die Verarbeitung erfolgt. Deshalb ist es wichtig, dass er über sämtliche möglichen Verarbeitungsorte vorab informiert wird. EU-Recht ist in diesem Zusammenhang bereits dann anwendbar, wenn der Cloud-Anwender als im Regelfall für die Verarbeitung verantwortliche Stelle im Rahmen der Tätigkeiten einer in der EU gelegenen Niederlassung personenbezogene Daten verarbeitet oder wenn die für die Verarbeitung verwendeten Mittel im Hoheitsgebiet der EU gelegen sind.[17]

3.4.1
Innereuropäischer Raum

Für Clouds im innereuropäischen Raum, bei denen die Datenverarbeitung ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR) stattfindet, ergeben sich dabei keine Besonderheiten. Aufgrund des weitgehend innerhalb des EWR harmonisierten Datenschutzniveaus gelten für alle Cloud-Anwender, -Anbieter und Unter-Anbieter dieselben datenschutzrechtlichen Anforderungen nach der Richtlinie 95/46/EG. Durch vertragliche

[17] vgl. Art.-29-Datenschutzgruppe, WP 179, S. 27

Vereinbarungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter muss der Ort der technischen Verarbeitung personenbezogener Daten vereinbart werden. Cloud-Anbieter sowie Unter-Anbieter können so verpflichtet werden, nur technische Infrastrukturen zu verwenden, die sich physikalisch auf dem Gebiet des EWR befinden.[18] Es ist daher nicht hinnehmbar, dass der Cloud-Anbieter eine Auskunft zu den Standorten der Datenverarbeitung verweigert, keinesfalls dürfte bei einer Verweigerung pauschal von einer Cloud im innereuropäischen Raum ausgegangen werden.

3.4.2 Außereuropäischer Raum

Erfolgen die Datenverarbeitungen allerdings außerhalb der EU und des EWR, indem die Cloud-Anbieter und/oder Unter-Anbieter eine Datenverarbeitung in Drittstaaten vornehmen, so gelten die besonderen Anforderungen der §§ 4b, 4c BDSG für den Drittstaatentransfer. Falls in dem Drittstaat kein angemessenes Datenschutzniveau besteht,[19] müssen daher durch den Cloud-Anwender als verantwortliche Stelle ausreichende Garantien zum Schutz des allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorgewiesen werden. Die Garantien können sich aus Standardvertragsklauseln oder u. U. aus Binding Corporate Rules ergeben.[20] In jedem Fall ist ein besonderes Augenmerk auf die Festlegung eines technischen und organisatorischen Datenschutzes zu legen (Kapitel 4).

Im Rahmen des Datentransfers mit Drittstaaten erlangen die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG vom 05.02.2010[21] an Bedeutung. Demnach agiert der Cloud-Anwender als verantwortliche Stelle und Datenexporteur, der Cloud-Anbieter hingegen als Datenimporteur, sofern er in einem Drittstaat ansässig ist.[22]

Gibt der im Drittstaat ansässige Cloud-Anbieter Daten an einen Unter-Anbieter, der ebenfalls seinen Sitz im außereuropäischen Raum hat, so wird Ersterer als Übermittler mitverantwortlich für die Rechtmäßigkeit der Datenübermittlung und -verarbeitung. Gleichwohl verbleibt eine Verantwortlichkeit des Cloud-Anwenders. Der Cloud-Anwender bleibt in jedem Fall haftungsrechtlich für sämtliche Schäden verantwortlich, die der Cloud-Anbieter oder Unter-Anbieter den Betroffenen zufügen.

Im Rahmen der durch eine Entscheidung der EU-Kommission erlassenen Standardvertragsklauseln, die vom Cloud-Anwender und Cloud-Anbieter unverändert übernommen werden müssen,[23] wurden allerdings die spezifischen Regelungen der Auftragsdatenverarbeitung nicht vollständig abgebildet, obwohl die vertraglichen und faktischen Beziehungen zwischen Datenexporteur und Datenimporteur einer solchen Verarbeitung ähnlich sind. Aus diesem Grunde muss der Cloud-Anwender über die Vereinbarung von Standardvertragsklauseln hinaus die Anforderungen nach § 11 Abs. 2 BDSG erfüllen und entsprechend vertraglich abbilden. Dies kann durch Regelungen in den Anlagen zum Standardvertrag und/oder ergänzende geschäftsbezogene Klauseln oder durch separate vertragliche Regelungen erfolgen, die nicht inhaltlich von den Standardvertragsklauseln abweichen.[24]

Solche Regelungen dienen der Wahrung der schutzwürdigen Belange der Betroffenen und können dazu führen, dass die Übermittlung durch den Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt ist.

Da aufgrund der Begriffsbestimmung in § 3 Abs. 4 Nr. 3 in Verbindung mit § 3 Abs. 8 BDSG die privilegierende Wirkung der Auftragsdatenverarbeitung nicht greift, wenn der Datenverarbeitungsdienstleister seinen Sitz außerhalb der EU und des EWR hat, und die Datenweitergabe an einen „Datenverarbeiter“ in einem Drittstaat also eine Übermittlung darstellt,[25] bedarf sie als solche einer Rechtsgrundlage. § 28 Abs. 1 Satz 1 Nr. 2 BDSG kann als Rechtsgrundlage in Betracht kommen. Im Rahmen der danach vorzunehmenden Interessenabwägung ist zu berücksichtigen, welche Rolle dem Datenempfänger im Drittstaat zukommt und welche Regelung der Datenexporteur mit diesem geschlossen hat. Wenn der Datenexporteur mit dem Datenimporteur einen Vertrag mit Festlegungen entsprechend § 11 Abs. 2

[18] Über eine Regionalgarantie hinaus ist auch eine Bindung an EU-Recht zwingend.
[19] Siehe hierzu die Entscheidungen der EU-Kommission: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.
[20] Es sollte immer auch die Option eines individuellen Vertrages erwogen werden.
[21] Entscheidung der EU-Kommission: siehe Endnote 19; zur Auslegung und Umsetzung dieser Entscheidung siehe die FAQs in WP 176 der Artikel 29-Gruppe: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm
[22] Näheres siehe WP 176 der Artikel 29 Gruppe (Endnote 21). Hier ist u. a. die Frage behandelt, inwieweit der Standardvertrag angewendet werden kann, wenn sich nur der Unterauftragnehmer (hier: Unter-Anbieter) im Drittstaat befindet, der Auftragneh¬mer (hier:Cloud-Anbieter) aber noch innerhalb der EU/des EWR
[23] Werden die EU-Standardvertragsklauseln geändert und wird dadurch ein individueller Vertrag geschaffen, so darf der Drittstaatentransfer nur erfolgen, wenn die zuständige Datenschutzaufsichtsbehörde die dann erforderliche Genehmigung gemäß § 4c Abs. 2 BDSG erteilt hat. Geringfügige Ergänzungen, die ausschließlich der Erfüllung der Voraussetzungen des § 11 Abs. 2 BDSG dienen, lösen noch keine Genehmigungspflicht aus. Näheres hierzu: Tätigkeitsbericht der Hessischen Landesregierung für die Datenschutzaufsicht im nicht öffentlichen Bereich für das Jahr 2009, Nr. 11.1, sowie Synopse der Datenschutzaufsichtsbehörden zu § 11-EU-Standardverträge (www.datenschutz.hessen.de)
[24] Näheres siehe Synopse, Endnote 23
[25] Dies ist eine Besonderheit des BDSG. Nach der Richtlinie 95/46/EG und den Datenschutzgesetzen anderer europäischer Länder gelten auch Datenverarbeitungsdienstleister in Drittstaaten als Auftragsdatenverarbeiter.

BDSG geschlossen hat, kann dies dazu führen, dass die Datenübermittlung aufgrund der Interessenabwägung gerechtfertigt ist.

Dies gilt freilich nur, soweit der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG überhaupt einschlägig sein kann.[26] Soweit besondere Arten personenbezogener Daten betroffen sind, scheidet das Cloud-Computing daher regelmäßig aus, denn § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist grundsätzlich nicht anwendbar und die Voraussetzungen der speziellen Erlaubnistatbestände nach § 28 Abs. 6 bis 9 BDSG dürften grundsätzlich nicht erfüllt sein.[27]

Erfolgt eine Verarbeitung personenbezogener Daten durch einen Cloud-Anbieter oder Unter-Anbieter mit Sitz in den USA, so können die EU-Standardvertragsklauseln ebenso wie Binding Corporate Rules entbehrlich sein, wenn sich der Cloud-Anbieter zur Einhaltung der Safe-Habor-Grundsätze verpflichtet hat. Cloud-Anbieter oder Unter-Anbieter mit Sitz in den USA können sich dabei auf freiwilliger Basis gegenüber dem US-Handelsministerium selbst zertifizieren, indem sie eine Beitrittserklärung unterzeichnet und deine Datenschutzerklärung veröffentlicht haben. Solange jedoch eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindeskriterien zu prüfen, bevor sie personenbezogene Daten an eine auf der Safe-Harbor-Liste geführtes US-Unternehmen übermitteln.[28] Daher ist zu fordern, dass sich der Cloud-Anwender mindestens davon überzeugt, ob das Zertifikat des Cloud-Anbieters noch gültig ist und sich auf die betreffenden Daten bezieht.[29] Soweit EU-Personaldaten verarbeitet werden sollen, muss der Cloud-Anwender ferner prüfen, ob der Cloud-Anbieter sich gemäß FAQ 9 Frage 4 des Safe-Harbor-Abkommens zur Zusammenarbeit mit den EU-Datenschutzaufsichtsbehörden verpflichtet hat.[30] Ferner muss der Cloud-Anwender prüfen und mit dem Cloud-Anbieter im Innenverhältnis sicherstellen, dass er (der Cloud-Anwender) bei einer Anfrage durch einen Betroffenen auch die nötigen Informationen erhält, um die Anfrage beantworten zu können.

Bestehen für den Cloud-Anwender Zweifel an der Einhaltung der Safe-Harbor-Grundsätze durch den Cloud-Anbieter, so sollte auf Standardvertragsklauseln oder Anbieter mit Binding Corporate Rules zurückgegriffen werden.[31]

Zu beachten ist, dass auch eine gültige Safe-Harbor-Zertifizierung des Cloud-Anbieters (und ggf. des Unter-Anbieters) den Cloud-Anwender nicht von dem Erfordernis befreit, schriftliche Vereinbarungen entsprechend § 11 Abs. 2 BDSG zu treffen. Auch in der Antwort zu FAQ 10 zu den Safe-Harbor-Grundsätzen wird klargestellt, dass vertragliche Regelungen entsprechend dem nationalen Datenschutzrecht des Datenexporteurs durch die Safe-Harbor-Zertifizierung nicht entbehrlich werden.

Die weiteren obigen Ausführungen zum Erfordernis einer Rechtsgrundlage für die Übermittlung (insbesondere die Problematik, falls § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht einschlägig sein kann) sind ebenfalls zu beachten.

Ebenso wenig entbindet die bloße Safe-Harbor-Zertifizierung den Cloud-Anwender von seiner Kontrollpflicht analog § 11 Abs. 2 Satz 3 BDSG. Die bloße Prüfung der Safe Harbor Zertifizierung genügt regelmäßig nicht den oben (3.2) dargestellten Anforderungen.

Beim Drittstaatentransfer können bei konzernangehörigen Auftragnehmern die erforderlichen ausreichenden Garantien zum Schutz der Persönlichkeitsrechte – wie bereits oben erwähnt – durch Binding Corporate Rules geschaffen werden. Wenn Cloud-Anwender und Cloud-Anbieter derselben Unternehmensgruppe angehören, sind Binding Corporate Rules selbstverständlich ohne weiteres möglich.

Auch hier wäre zu beachten, dass Binding Corporate Rules den Cloud-Anwender nicht von dem Erfordernis befreien, schriftliche Vereinbarungen entsprechend § 11 Abs. 2 BDSG zu treffen.[32] Es besteht ebenfalls das Erfordernis einer Rechtsgrundlage für die Übermittlung.

[26] Soweit öffentliche Stellen Cloud Services in Drittstaaten anwenden, ist hier eine besonders sorgfältige Prüfung geboten, denn ein dem § 28 Abs. 1 Satz 1 Nr. 2 BDSG entsprechender Erlaubnistatbestand dürfte es in den Landesdatenschutzgesetzen nicht geben, soweit ersichtlich. Die Verfasser dieser Orientierungshilfe haben allerdings keine Prüfung aller Landesdatenschutzgesetze vorgenommen.

[27] § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist auch nicht einschlägig, wenn es sich um Daten handelt, die dem TKG unterfallen (Problematik des § 92 TKG, der aber geändert werden soll, um Auftragsdatenverarbeitung in Drittstaaten zu ermöglichen). Gleiches dürfte für TMG-Daten gelten. Auch bei Personaldaten ist streitig, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG einschlägig sein kann. Hier sind letztlich die Regelungen in der geplanten BDSG-Novelle maßgeblich.

[28] Siehe dazu Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010).

[29] Diese Prüfung kann anhand der Eintragungen in der Safe-Harbor-Liste erfolgen: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (Siehe auch Tätigkeitsbericht der Hessischen Landesregierung für die Datenschutzsicht im nicht öffentlichen Bereich für das Jahr 2007 Nr. 10, abrufbar unter: http://www.datenschutz.hessen.de)

[30] Auch dies kann anhand der Eintragungen in der Safe-Harbor-Liste geprüft werden.

[31] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 28./29.04.2010 in Hannover; Prüfung der Selbstzertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen.

[32] Siehe auch WP 153 Nr. 6.1und WP 154 Nr. 11 und 12 der Artikel 29-Gruppe: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm

4 Technische und organisatorische Aspekte

Cloud-Computing-Systeme der Cloud-Anbieter unterliegen bestimmten infrastrukturellen Rahmenbedingungen, deren Schutz bezüglich der Grundwerte Verfügbarkeit, Vertraulichkeit, Integrität, Revisionssicherheit und Transparenz (nähere Definitionen siehe Kapitel 4.1.1) gewährleistet werden muss.

Dieser Schutz orientiert sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten. Die Umsetzung der Schutzziele ist durch technische und organisatorische Maßnahmen abzusichern.

Kapitel 4.1.2 beschreibt die grundsätzlichen cloudspezifischen Risiken und in Kapitel 4.1.3 werden die klassischen Risiken, die ein Erreichen der Schutzziele erschweren, näher erläutert.

In den nachfolgenden Kapiteln 4.2–4.4 werden anhand der beschriebenen Schutz-ziele für die verschiedenen Betriebsmodelle IaaS, PaaS, SaaS die Risiken spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

4.1
Ziele und Risiken

4.1.1
Schutzziele

Die Grundwerte sind wie folgt definiert:

Verfügbarkeit:
Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß von autorisierten Benutzern verarbeitet werden.

Vertraulichkeit:
Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.

Integrität:
Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell. Die Funktionsweise der Systeme ist vollständig gegeben.

Revisionssicherheit:
Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Transparenz:
Die Verfahrensweise bei der Verarbeitung personenbezogener Daten ist vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden kann.

4.1.2
Cloudspezifische Risiken

Eine zentrale Eigenschaft des Cloud Computing ist, dass Computerressourcen von den Cloud-Anwendern genutzt werden, auf die sie selbst keinen konkreten Zugriff haben. Es ist in der Regel nicht nachvollziehbar, wo und auf welchen Systemen Anwendungen und Daten gespeichert sind, ausgeführt oder verarbeitet werden, besonders dann, wenn der Anbieter des Cloud Computing seine Dienstleistungen und Services (teilweise) bei anderen Anbietern einkauft und dieses nicht transparent für den Cloud-Anwender geschieht.

Daraus resultieren die meisten Risiken, die folgende Aspekte betreffen:

Löschung von Daten
Das Löschen im Sinne des endgültigen Unkenntlichmachens von Daten kann bei Anwendungen des Cloud Computing nicht ohne Weiteres realisiert und überprüft werden. So besteht für den Cloud-Anwender die Unsicherheit, ob

- eine vollständige Löschung seiner Daten erfolgt, wenn er ein entsprechendes Kommando absetzt;
- die Daten am vorherigen Ort zuverlässig und sicher gelöscht werden oder vor dem Zugriff späterer Anwender sicher geschützt sind, wenn der Cloud-Anbieter den Ort der Erbringung der Dienstleistungen aus eigenen Erwägungen verlagert.

Nachvollziehbarkeit durch Protokollierung und Dokumentation

- Die meisten Protokolle und Dokumentationen zur Datenverarbeitung in der Cloud befinden sich beim Cloud-Anbieter, so dass die darauf aufbauende Kontrolle nicht durch den verantwortlichen Cloud-Anwender, sondern nur durch den Cloud-Anbieter erfolgen kann. Während der Cloud-Anwender kaum über regelmäßige Reports, Informationen über Schwierigkeiten und wichtige Vorfälle sowie über System-und Nutzungsprotokolle verfügt, kontrolliert sich der Cloud-Anbieter allenfalls selbst.

Vervielfältigung und Verteilung der Daten

- Anwender von Cloud Computing haben in der Regel keine Gewissheit, wo auf der Welt ihre Anwendungen laufen bzw. ihre Daten verarbeitet werden. Die Verarbeitung und Speicherung kann auch fragmentiert und damit verteilt geschehen, insbesondere dann, wenn der Cloud-Anbieter Teile seines Portfolios bei anderen Anbietern bezieht.
- Anbieter von Cloud-Services sind gemeinhin an Standorten angesiedelt, die über extrem breitbandige Internet-Anbindungen verfügen. Diese leistungsfähigen Anbindungen sind notwendig, um überhaupt Cloud-Services anbieten zu können; sie ermöglichen es aber auch, in kürzester Zeit auch große Datenmengen an andere Standorte zu verschieben oder zu kopieren.

Sorgfältige Einführung von Cloud-Lösungen

Cloud-Services können oft innerhalb sehr kurzer Zeiträume bereitgestellt werden. Sie sind in der Regel vorkonfiguriert und können schnell in Betrieb genommen werden. Dies kann dazu verleiten, neue Verfahren zur Verarbeitung personenbezogener Daten ohne die erforderliche Sorgfalt einzurichten, indem insbesondere

- nicht oder nur oberflächlich geprüft wird, ob bzw. unter welchen Bedingungen die vorgesehene Verarbeitung rechtlich zulässig ist;
- Systeme nicht schrittweise mit sorgfältig ausgewählten Testdaten, sondern mit Echtdaten getestet werden.

4.1.3 Klassische Risiken

Cloud-Computing-Systeme unterliegen ebenso wie klassische IT-Systeme bestimmten Rahmenbedingungen, deren Schutz bezüglich der Grundwerte Verfügbarkeit, Vertraulichkeit, Integrität, Revisionssicherheit und Transparenz gewährleistet werden muss.

Die Umsetzung dieser Schutzziele kann auch in der Cloud in Frage gestellt werden durch

- versehentliches oder vorsätzliches Handeln von Mitarbeitern und Unter-Anbietern des Cloud-Computing-Providers, z. B. durch unberechtigtes Kopieren oder Klonen von Systemen, unberechtigte Manipulation oder Herunterfahren von Virtuellen Maschinen, Herunterfahren von Hosts, unberechtigte Manipulation von Konfigurationsdateien;
- Nutzung von Sicherheitslücken beim Provider durch andere Kunden, z. B. zur Übernahme der Kontrolle über andere Virtuelle Maschinen,

durch Zugriff auf das Dateisystem des Host, zu Denial-of-Service-Angriffe auf den Hypervisor, zum Abhören der Datenkommunikation zwischen Virtuellen Maschinen, durch unberechtigte Speicherzugriffe;
- Nutzung von Sicherheitslücken durch Angriffe Dritter;
- Missbrauch der Plattform des Providers, z. B. für Brute-Force-Angriffe auf Passwörter, den Aufbau von Botnetzen, die Einschleusung von Schadsoftware, das Versenden von SPAM;
- Nutzung von Sicherheitslücken auf den Übertragungswegen via Internet zwischen Kunden und Providern;
- Nutzung von Sicherheitslücken in den vom Provider zur Nutzung durch die Kunden bereit gestellten Software-Schnittstellen und APIs;
- Angriffe durch Schadsoftware auf die Dienste in der Cloud;
- Risiken jeglicher Form von Computerkriminalität durch schlecht kontrollierte Registrierungsmodalitäten zur Nutzung von Cloud-Diensten;
- Cloud-unabhängige Sicherheitsmängel der technischen Infrastruktur – bedingt durch fehlende oder unzureichende Sicherheitskonzepte, wie z. B. eine unsichere Stromversorgung, eine mangelhafte Klimatisierung der Infrastrukturräume oder die Zutrittskontrolle zu Gebäuden und Räumen;
- missbräuchlichen Umgang mit Datensicherungen, indem korrekt gelöschte Daten aus Backupsystemen ggf. an unterschiedlichen Verarbeitungsorten rekonstruiert werden;
- mangelhafte Löschung defekter Speichermedien vor deren Austausch oder Aussonderung.

Datentrennung

Die unter Umständen schwierige Kontrolle des Zugriffs auf Daten und Anwendungen bei der Nutzung von Cloud-Services kann dazu führen, dass

- Cloud-Anwender so genannter virtueller Maschinen (VM) die Ressourcennutzung anderer auf dem Rechner befindlicher VM ausspionieren und darüber weitere Aktivitäten zum unbefugten Zugriff auf die in den anderen VM gespeicherten und verarbeiteten Daten entwickeln können;
- wegen der Teilung der verfügbaren Ressourcen zwischen vielen Cloud-Anwendern Risiken bestehen, da die Daten verschiedener Kunden nicht hinreichend getrennt verarbeitet werden;[33]

[33] Dies ist insbesondere dann der Fall, wenn die gleiche Datenbankinstanz aus Kostengründen für verschiedene Cloud-Anwender eingesetzt wird und damit auf Datenseparierung verzichtet wird. Letzteres kann auch dann der Fall sein, wenn die zu teilenden Ressourcen und der Virtualisierungs-Hypervisor nicht optimal aufeinander abgestimmt sind.

- letzteres auch dann der Fall sein kann, wenn die zu teilenden Ressourcen und der Virtualisierungs-Hypervisor nicht optimal aufeinander abgestimmt sind.

Transparenz der Datenverarbeitung in der Cloud
Die Transparenz der Datenverarbeitung in der Cloud ist für die aus der Ferne arbeitenden Cloud-Anwender ohne besondere Maßnahmen des Cloud-Anbieters kaum gegeben. Dies führt u. U. dazu, dass

- die Cloud-Anwender die Kontrolle über den Zugriff auf die eigenen Daten aufgeben, wenn das Personal des Cloud-Anbieters zu allen Daten Zugang hat, die in der Cloud verarbeitet werden;
- bei der Nutzung einer Public Cloud in Drittländern der Zugriff auf Daten des Cloud-Anwenders durch staatliche und private Stellen möglich und nicht kontrollierbar ist;
- Cloud-Anwender nicht über den Ort der Verarbeitung oder die Wege ihrer Daten durch die Cloud und die näheren Umstände der Verarbeitung beim Cloud-Anbieter informiert werden;
- Cloud-Anwender nicht kontrollieren können, ob die Umstände der Datenverarbeitung und die Maßnahmen zum organisatorischen Datenschutz beim Cloud Computing Anbieter den Verträgen zur Auftragsdatenverarbeitung (§ 11 BDSG) gerecht werden;
- Cloud-Anwender keine Kontrolle über die Datenspuren haben, die sie bei der Nutzung der Cloud hinterlassen;
- Cloud-Anwender keine Kontrolle über Unter-Anbieter der Cloud-Anbieter haben, denen der Zugriff auf die Rechner ermöglicht wird.

Verfügbarkeit in der Cloud
Die Verfügbarkeit der über die Cloud angebotenen Dienstleistung kann gefährdet werden durch

- Leistungsverweigerung durch betrügerisches Handeln des Cloud-Anbieters;
- Ausfall der Hardware des Providers (spontan, etwa durch Softwarefehler in den komplexen Plattformen, durch Fehler oder vorsätzliches Handeln von Mitarbeitern des Providers, durch Angriffe von außen, z. B. bei DDoS-Angriffen durch Botnetze, Beschädigung von Speichermedien bei fehlendem Back-up);
- Ausfall der Dienste und Anwendungen oder Löschung von Daten durch versehentliches oder vorsätzliches Handeln von Mitarbeitern und von Unter-Anbietern des Cloud-Anbieters, z. B. durch unberechtigtes Herunterfahren einer Virtuellen Maschine oder eines Hosts;

- die spontane, versehentlich oder absichtlich bewirkte Unterbrechung von Verbindungen zwischen Netzelementen, z. B. in der Verbindung zwischen Kunden und Provider, auch bewirkt durch die bei Cloud Computing erhöhte Komplexität der Netze;
- Mängel des Qualitätsmanagements bei Vorbereitung und Betrieb der Cloud-Anwendungen, die zu Ausfällen der Provisionierung (Bereitstellung), fehlerhaften Betriebsmittel-Reservierungen, Konfigurationsfehlern sowie Fehlern beim System-Upgrade führen können;
- technische Störungen der Kommunikationskanäle eines Cloud-Anwenders, die nicht nur die Kommunikation, sondern auch die Geschäfts-und Produktionsprozesse beeinträchtigen;
- die erschwerte Erstellung von Backups sowie die Intransparenz des Backup und die Abhängigkeit vom Anbieter dabei;
- Angriffe durch Schadsoftware auf die Dienste in der Cloud.

In den folgenden Kapiteln werden anhand der beschriebenen Schutzziele für die verschiedenen Betriebsmodelle die Risiken spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

4.2
Infrastructure as a Service (IaaS)

Cloud-Anbieter, deren Dienste IaaS-Angebote beinhalten, stellen essentielle IT-Ressourcen zur Verfügung. Diese beinhalten im Wesentlichen Speicherressourcen, Rechenleistung und Kommunikationsverbindungen, die meist virtualisiert in einem Cloud-Computing-System von einem oder mehreren Anbietern bedarfsgerecht zur Verfügung gestellt werden. Ein direkter Zugriff auf die zum Anbieten des Dienstes genutzten Systemkomponenten ist nicht möglich. Alle Kernkomponenten liegen ausschließlich im Einflussbereich des Anbieters. Dennoch muss sich der Cloud-Anwender als Auftraggeber für die Datenverarbeitung über den Stand der Informationssicherheit selbst überzeugen können. Dazu sollte der Anwender die Möglichkeit erhalten, die Seriosität der Cloud-Anbieter verifizieren zu können, indem unabhängige Stellen Zertifikate für datenschutzkonforme Anbieter erteilen dürfen.

Alle Maßnahmen auf der Ebene des IaaS, die zum Erreichen der einzelnen Schutz-ziele dienen, liegen in der Verantwortung des Cloud-Anbieters und sollten sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten orientieren. In diesem Zusammenhang sind Kumulationseffekte auf Grund der systemimmanenten offenen Struktur, die an einer Vielzahl von Anwendern ausgerichtet ist, zu beachten.

Wie können auf der Ebene des IaaS die grundsätzlichen datenschutzrechtlichen Anforderungen

technisch umgesetzt werden?

Infrastrukturelle Gegebenheiten (z. B. physikalische Sicherheit)
Der Schutz der infrastrukturellen Gegebenheiten umfasst alle technischen und organisatorischen Maßnahmen, die auf den Schutz der Liegenschaft, insbesondere der Gebäude und Räume, in denen die zu betrachtenden IT-Komponenten aufgestellt sind, gerichtet sind. Dazu zählt z. B. eine sichere Stromversorgung, Aspekte des Brandschutzes und der Klimatisierung, Zugangs-, Zutritts-und Zugriffssicherungssysteme sowie Redundanzen essentieller Komponenten.

Vertraulichkeit, Verfügbarkeit
Eine typische Gefährdung für die Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und deren personenbezogener Daten basiert auf dem Diebstahl und Ausfall von nicht redundanter Hardware (z. B. Speichermodule oder Rechner), die sich im Einflussbereich des Cloud-Anbieters (Ressourcen-Anbieter) befinden.

IT-Systeme (z. B. Host, Speicher)
Die Prozesse in der Cloud und deren Berechnungen werden auf den IT-Systemen (Hardware) des Ressourcen-Anbieters ausgeführt und müssen ebenfalls angemessen abgesichert werden. Dazu zählen z. B. Zugriffsbeschränkungen, Patchmanagement, sichere Grundkonfiguration, Sicherheitsrichtlinien, Integritätsprüfung, revisionssichere Protokollierung, Datensicherung, Intrusion-Detection-Systeme (IDS), Firewalls und Virenschutz.

Vertraulichkeit, Integrität, Verfügbarkeit
Der Cloud-Anwender wird mittels der Virtualisierungstechnologie daran gehindert, direkt auf die Hardware-Ebene durchzugreifen. Diese Isolation kann die Etablierung einer sicheren Umgebung begünstigen.

Als besonders schützenswert ist der Cloud-Operator (Cloud Control) zu betrachten, da dieser die zur Verfügung gestellten Ressourcen koordiniert und dem Nutzer bedarfsgerecht zur Verfügung stellt.

Netze (z. B. Kommunikationsverbindungen)
Die Kommunikationsverbindungen zwischen den Cloud-Ressourcen sowie den Cloud-Anwendern stellen zentrale Komponenten dar, die bezüglich der

Schutzziele, insbesondere der Vertraulichkeit und Verfügbarkeit, abgesichert werden müssen.

Vertraulichkeit
Die Vertraulichkeit personenbezogener Daten ist zu wahren, indem zu deren Schutz kryptographische Verfahren (Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationspartnern) eingesetzt werden. Dies betrifft insbesondere die für die Administration eingerichteten Fernwartungszugänge.

Netzbasierte Angriffe können mittels Intrusion-Detection-Systeme (IDS) und Intrusion-Prevention-Systeme (IPS) ermittelt bzw. verhindert werden, um mit speziell abgestimmten Maßnahmen reagieren zu können.

Verfügbarkeit
Da die Verfügbarkeit ein wesentlicher Aspekt netzbasierter Maßnahmen darstellt, sollten die Kommunikationsverbindungen zwischen den Rechenzentren sowie deren Anbindung an das Netz redundant ausgelegt sein.

Virtualisierung
Cloud-Systeme zeichnen sich durch die Verwendung der Virtualisierung aus, hierbei werden dem Cloud-Anwender virtualisierte Ressourcen (z. B. virtueller Speicher, virtuelle Maschinen) zur Verfügung gestellt. Die physischen Ressourcen werden dabei mittels einer Virtualisierungssoftware (Virtual Machine Monitor-VMM oder Hypervisor) abstrahiert. Die damit einhergehende Steigerung der Komplexität (jede virtuelle Maschine benötigt ein Server-, Storage-und Netzwerkkonzept) erhöht auch die Komplexität der Sicherheitsanforderungen und bedarf zusätzlicher, der Technologie geschuldeter Sicherheitsuntersuchungen (z. B. Verschiebung (VMotion) und Snapshots virtueller Maschinen). Des Weiteren unterliegen Virtualisierungen besonderen Bedingungen bei den Bereitstellungsmechanismen von CPU und RAM sowie der Storage-und Netwerk-Anbindung, die einer gesonderten Risikoanalyse bedürfen.

Transparenz
Der Cloud-Anwender sollte auf die Veröffentlichung von Benutzerrichtlinien zur Absicherung der virtuellen Systemlandschaft des Cloud-Anbieters achten. Der Einsatz zertifizierter Virtualisierungssoftware erhöht neben der Sicherheit auch die Transparenz des verwendeten Systems und schafft Vertrauen bei den Anwendern.

Integrität/Vertraulichkeit
Eine besondere Bedeutung kommt dem sensitiven administrativen Zugang zu diesen Maschinen zu, da dieser in der Regel über öffentliche Netze läuft

und dementsprechend abgesichert werden muss. Ferner sollte ein durchdachtes Rechte-und Rollenkonzept für diese Zugänge geschaffen werden.

4.3
Platform as a Service (PaaS)

Bietet ein Cloud-Anbieter PaaS-Dienste an, so bietet er Infrastrukturen zur Entwicklung von Cloud-Anwendungen an. In diesen Entwicklungsumgebungen, die auch als technische Frameworks oder Laufzeitumgebungen bezeichnet werden, können Cloud-Anwender eigene Anwendungen entwickeln.

Die Entwicklungsumgebung bietet technische Funktionen, wie Datenbanken und Werkzeuge, die es den Anwendern ermöglicht, gleichzeitig an Programmen, Dokumenten und Daten zu arbeiten.

Grundlegende Einstellungen an diesen Infrastrukturen können in der Regel vom Cloud-Anwender nicht oder nur in sehr begrenztem Umfang durchgeführt werden. Diese administrative Hoheit liegt daher beim Cloud-Anbieter. Da die Anwender die Anwendungen selbst entwickeln, haben sie direkten Einfluss auf diese und somit auf die Art und Weise, wie Daten innerhalb der Anwendungen und der Laufzeitumgebungen verarbeitet werden. Die datenschutzrechtliche Verantwortung für diese Daten liegt bei den Cloud-Anwendern.

Bei der Entwicklung der Anwendungen ist der Grundsatz der Datensparsamkeit zu beachten (§ 3a BDSG). Dies gilt sowohl für die innerhalb der Anwendung zu verarbeitenden Daten als auch für eventuelle Protokoll-Daten, die von den selbst entwickelten Anwendungen oder den dabei eingesetzten Funktionalitäten der PaaS-Umgebung erzeugt werden.

Wie bei allen Cloud-Services gilt es, genaue vertragliche Regelungen (Verträge nach § 11 BDSG bzw. in Standardverträgen und ggf. in separaten Verträgen, im folgenden vereinfachend insgesamt auch als Service Level Agreements bezeichnet, SLA) zwischen Cloud-Anbieter und Anwender festzulegen, um weitestgehende Kontrolle des Anwenders über die Datenverarbeitung in der Cloud zu realisieren. Ändert der Cloud-Anbieter Bestandteile seiner PaaS-Umgebungen, so darf das nur mit voriger Information – in Einzelfällen auch nur mit Zustimmung – des Cloud-Anwenders passieren.

Die Kontroll-und Regelungsmöglichkeiten sind von immenser Wichtigkeit, um die gesetzlichen Anforderungen bezüglich des Datenschutzes an den Auftraggeber (hier Cloud-Anwender) erfüllen zu können. Die Anforderungen

können nur bei ausreichender Transparenz, das heißt durch einen wohl informierten Kunden, wahrgenommen werden. Wohl informiert bedeutet in diesem Fall, dass der Cloud-Anwender Hilfsmittel an die Hand bekommt, mit denen er sich von der datenschutzkonformen und vertragsgemäßen Verarbeitung personenbezogener Daten überzeugen kann. Diese Hilfsmittel können sowohl technischer als auch organisatorischer Natur sein.

Transparenz

Cloud-Anwendern ist es in der Regel nicht oder nur selten möglich, sich direkt bei den Cloud-Anbietern von der vertragsgemäßen Verarbeitung der Daten zu überzeugen. Die Daten und Anwendungen können zeitgleich über eine Vielzahl von geografisch getrennten Standorten verteilt sein. Eine Vor-Ort-Kontrolle wird dadurch unmöglich. Es ist daher zwingend notwendig und vertraglich zu regeln, dass der Cloud-Anbieter alle möglichen Unter-Anbieter sowie alle Standorte bekannt gibt, an denen die Verarbeitung stattfindet bzw. im Rahmen des Vertragsverhältnisses stattfinden könnte. Dazu gehören insbesondere auch die Standorte der Unter-Anbieter. In diesem Zusammenhang ist darauf hinzuweisen, dass der Cloud-Anbieter für die Datenverarbeitung der Unter-Anbieter haftet, aber mit zunehmender Anzahl von eingebundenen Unter-Anbietern selbst das Problem hat, die Kontrolle über die Daten zu verlieren.

Dem Problem schwieriger Überprüfbarkeit der vertragsgemäßen Verarbeitung der Daten kann unter Umständen dadurch begegnet werden, dass lediglich Angebote von Cloud-Anbietern genutzt werden, die regelmäßig von unabhängigen Stellen auditiert und zertifiziert werden. Unabhängige Stellen können die Korrektheit der entsprechenden Verfahren zu einem Prüfzeitpunkt bestätigen. Zusätzlich ist es für die Transparenz gegenüber dem Anwender von Vorteil, wenn der Anbieter von Cloud-Diensten regelmäßig Berichte über das Sicherheitsumfeld zu den Diensten veröffentlicht. Bei akuten Vorfällen ist eine unverzügliche und aussagekräftige direkte Information der Cloud-Anwender erforderlich.

Ein den deutschen Datenschutzanforderungen völlig gleichwertiges Datenschutzniveau ist lediglich dann gewährleistet, wenn personenbezogene Daten ausschließlich innerhalb der EU oder EWR-Vertragsstaaten stattfindet. Ein völlig gleichwertiges Niveau wird nicht erreicht, wenn die Daten in Unternehmen gespeichert und verarbeitet werden, die EU/EWR-fremden staatlichen Kontrollen unterstehen. Das betrifft sowohl personenbezogene Daten, die in den innerhalb der PaaS-Umgebungen zu entwickelnden Anwendungen verarbeitet werden, als auch personenbezogene Daten, die

in Protokolldaten anfallen. Protokolldaten können innerhalb der PaaS-

Umgebung anfallen, aber auch „außerhalb“ in den Systemprotokollen der Cloud-Anbieter.

Auch die Herausgabe von Richtlinien zur Erstellung von sicheren, datenschutzkonformen Anwendungen an die Cloud-Anwender kann dem Schutzziel Transparenz dienen.

Verfügbarkeit
Jeder Cloud-Anbieter muss – wie jedes herkömmliche Rechenzentrum – zwingend über eine funktionierende Sicherheitsarchitektur und das zugehörige Management verfügen. Idealerweise nutzt jeder Cloud-Anbieter nur entsprechend zertifizierte Rechenzentren.

Besonderes Augenmerk bei der Auswahl des Cloud-Anbieters muss der Cloud-Anwender grundsätzlich auch auf die Portabilität richten: Alle Inhalte der PaaS-Umgebung sollten ohne Probleme zu einem anderen Anbieter portierbar sein. Leider ist der Datenexport häufig nicht ohne größeren Aufwand möglich, da die Anwendungen in einem bestimmten Kontext entwickelt wurden. Portierbarkeit ist eine Vorsichtsmaßnahme, die besonders bei einer Insolvenz des Cloud-Anbieters zum Tragen kommt, wenn der PaaS-Dienst nicht aufrechterhalten werden kann. In diesem Zusammenhang kommt auch der Zugriffsmöglichkeit durch den Cloud-Anwender eine besondere Bedeutung zu: Der Anwender muss die Möglichkeit haben, auch im Rahmen einer Insolvenz des Anbieters auf seine Daten zuzugreifen und diese aus den Systemen des Anbieters beispielsweise auf die Systeme eines anderen Anbieters zu transferieren.

Eine (möglichst) geographisch verteilte, redundante Datenhaltung und -Verarbeitung ist in Hinblick auf die Verfügbarkeit in der Cloud von Vorteil, für die Transparenz von Nachteil. Eine leicht zu realisierende, geografisch vom jeweils aktuell genutzten Verarbeitungsstandort getrennte Datensicherung ist hinsichtlich der Verfügbarkeit notwendig. Wie immer im Zusammenhang mit Datensicherungen gilt: Werden Daten im Echtsystem ordnungsgemäß gelöscht, müssen diese auch aus den vorhandenen Datensicherungen irreversibel entfernt werden.

Revisionsfähigkeit
Im Hinblick auf die Transparenz ist für den Cloud-Anwender bei der Nutzung von PaaS eine revisionssichere Protokollierung erforderlich. Das betrifft in erster Linie die Protokoll-Systeme des Cloud-Anbieters. Die Anwender müssen in die Lage versetzt werden, Einsicht in eine lückenlose, unverfälschte Protokollierung zu erhalten, um etwaige unberechtigte Zugriffe auf personenbezogene Daten festzustellen und besonders auch um die Tätigkeiten des Anbieters in Bezug auf die SLA überprüfen zu können.

Weiterhin ist ein Konfigurationsmanagement seitens des Anbieters geboten, um sich selbst und auch den Anwender jederzeit in die Lage versetzen zu können, die jeweils aktuellen oder in der Vergangenheit in Betrieb befindlichen Cloud-Konfigurationen nachvollziehen zu können.

4.4
Software as a Service (SaaS)

Bei der Nutzung eines SaaS-Angebots nutzt der Cloud-Anwender die Infrastruktur, die Plattformen und Anwendungssoftware des Cloud-Anbieters. Die „Schnittstelle“ zwischen Anwender und Anbieter ist dabei weiter in die Sphäre des Anwenders und seiner konkreten Anwendungsbedürfnisse vorgerückt. Daher gelten die technischen und organisatorischen Anforderungen, die für die Betriebsformen Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) formuliert worden sind, für SaaS gleichermaßen. Zu den IT-Sicherheitsanforderungen, die der Anbieter mit seiner Infrastruktur und seinen Plattformen zu erfüllen hat, kommen zusätzliche verfahrensspezifische Anforderungen an eine sichere und ordnungsgemäß funktionierende Anwendung hinzu. Zwar wird der Anwender von seiner datenschutzrechtlichen Verantwortung für seine IT-Anwendungen nicht entbunden, seine Einflussmöglichkeiten im laufenden Betrieb sind jedoch auch für die Anwendungsprogramme minimal, weil er alles – sozusagen von der Stange – einkauft.

Da die Spielräume für das Customising bei Cloud-Anwendungen meist gering sind, muss der Anwender je nach Bedeutung und Tiefe der Anwendung[34] mehr oder weniger einschneidende Anpassungen seiner Strukturen und Geschäftsprozesse in Kauf nehmen. Weil er sich im laufenden Betrieb in großer Abhängigkeit vom Anbieter befindet, muss der Anwender seiner Verantwortung für die Anwendung vor Beginn der Cloud-Nutzung nachkommen und über die wichtigsten Anwendungsaspekte die Kontrolle behalten. Das wichtigste Schutzziel, dessen Erreichung der Anwender vom Anbieter verlangen muss, ist daher die Transparenz. Sie muss den Anwendern ermöglichen, mit den Anbietern anspruchsvolle Service Level Agreements (SLAs) zu vereinbaren, die es den Anbietern ermöglichen, ihre Verantwortung wahrzunehmen, schon um den hohen Compliance-Anforderungen nachzukommen.

Cloud-Dienste werden gewöhnlich mittels web-basierten Technologien (z. B. Webinterfaces für Anwender und zur Administration, client-seitige

[34] So wird zum Beispiel eine SaaS-Nutzung von Office-Anwendungen wie etwa bei Google Apps weniger Anpassungsbedarf benötigen als Personalinformationssysteme oder Kundenbindungssysteme (CRM).

Application Frameworks) zur Verfügung gestellt. Diese beinhalten Risiken für die in der Cloud zu verarbeitenden Daten, sofern die Prinzipien einer sicheren Software-Entwicklung auf Seiten des Cloud-Anbieters nicht eingehalten werden und der Cloud-Anwender sein Webinterface im Rahmen eines Sicherheitskonzepts, dem Schutzbedarf der Daten angemessen, nicht schützt.

Transparenz

Der Anwender ist verpflichtet zu prüfen, ob der Anbieter neben anderem auch hinreichende Garantien für die Sicherheit und Ordnungsmäßigkeit aller in der Cloud bereit gestellten Ressourcen anbietet und ob das Anwendungsverfahren hinsichtlich der Nutzung personenbezogener Daten den für den Anwender geltenden gesetzlichen Bestimmungen genügt. Dazu gehören sowohl die datenschutzrechtliche Zulässigkeit als auch die Beachtung des Gebots der Datensparsamkeit und die Umsetzbarkeit der Betroffenenrechte. Der Anwender muss dies durch bereit gestellte Dokumentationen und Protokolle nachvollziehen und ggf. nachweisen können. Dabei würde ihm helfen, wenn der Anbieter auch Zertifikate unabhängiger Stellen vorlegen kann, die die Konformität der Anwendungssoftware mit den datenschutzrechtlichen Bestimmungen versichern, die für den Anwender gelten.

Vertraulichkeit

Die Vertraulichkeit der Anwendungsdaten wird durch die Verhinderung des unbefugten Zugangs an Netz-, Speicher-und Verarbeitungskomponenten der Infrastruktur und des unbefugten Zugriffs auf die Daten sowie durch die Nutzung kryptografischer Verfahren bei der Übertragung und Speicherung der Daten gewährleistet (gemäß Nr. 2 der Anlage zu § 9 Satz1 BDSG). Die Sicherung des Zugangs zur Infrastruktur gehört ebenso zum Angebot des Anbieters wie auch die Bereitstellung kryptografischer Verfahren für die sichere Übertragung und Speicherung der Anwendungsdaten. Soweit der Anbieter die Verschlüsselung der Daten nicht obligatorisch vorsieht, ob er es also dem Anwender überlässt, bei der Übertragung der Daten zwischen Anwender und Anbieter und/oder bei der Speicherung in der Infrastruktur des Anbieters für eine Verschlüsselung der Daten zu sorgen, kann der Anwender insoweit selbst in Abhängigkeit vom Schutzbedarf seiner Daten für die angemessene Nutzung der Verschlüsselungsoptionen sorgen.

Ebenfalls liegen die Sicherheitsmaßnahmen an der Anwender-Anbieter-Schnittstelle in der Verantwortung des Anwenders. Dies gilt sowohl für die Nutzung der Systeme des Anwenders, von denen aus die Cloud-Anwendung betrieben wird, als auch für den Aufruf der Cloud-Anwendung über

diese Systeme, bei dem allerdings das von der Anwendungssoftware des Anbieters bereitgestellte Authentisierungsverfahren Verwendung findet.

Der Umgang mit den Authentisierungsmitteln, also mit Kennungen, Passwörtern, PINs, TANs, maschinenlesbaren Ausweisen und Token, ggf. auch biometrischen Merkmalen liegt in der Verantwortung des Anwenders.

Verfügbarkeit

Maßnahmen zu Absicherung der Verfügbarkeit einer SaaS-Anwendung liegen fast ausschließlich in der Hand des Anbieters. Der Schutz vor Angriffen auf die Verfügbarkeit der Infrastruktur (z. B. DDoS-Angriffe), der Plattformen und der Anwendungssoftware ist Teil der Dienstleistung, die in Verträgen verabredet wird.

Die Anwender sind für die Verfügbarkeit ihrer Seite der Anwender-Anbieter-Schnittstelle verantwortlich, also in der Regel für den PC, die Internetverbindung und den Webbrowser für den Zugang an die Cloud. Sofern die Datensicherung nicht Teil der Cloud-Dienstleistung ist, muss sie ferner vom Anwender über die Schnittstelle zur Cloud realisiert werden können.

Integrität

Die Integrität der Anwendungsdaten wird durch fehlerhafte bzw. nicht ordnungsgemäß gestaltete Verarbeitungsverfahren und durch unbefugte oder unbeabsichtigte Datenveränderungen gefährdet. Da bei SaaS die Verarbeitungsverfahren in der Verantwortung des Anbieters liegen, hat dieser Verfahrensmängel zu vermeiden bzw. zu beseitigen. Unbefugte Datenveränderungen können durch Angriffe auf die Infrastruktur und die Plattformen, z. B. durch unzuverlässige Mitarbeiter des Anbieters bewirkt werden und müssen durch Maßnahmen des Anbieters wirksam verhindert werden.

Aber auch seitens der Anwender kann der nachlässige oder vorsätzlich schädigende Umgang mit den eigenen Anwendungsdaten über die Cloud-Schnittstelle zu Integritätseinbußen führen. Hier liegt es nun wieder in der Verantwortung der Anwender, angemessene Maßnahmen zu ergreifen, damit dies nicht geschieht bzw. großer Schaden verhindert wird. Dabei wäre den Anwendern geholfen, wenn die vom Anbieter bereitgestellten Anwendungen geeignete Plausibilitätsprüfungen ermöglichen würden.

Revisionsfähigkeit

Das Schutzziel Revisionsfähigkeit wird durch die nachträgliche regelmäßige oder anlassbezogene Prüfung sicherheitsrelevanter Vorgänge bei der Datenverarbeitung erreicht. Diese Prüfung setzt voraus, dass die wichtigsten Angaben zu den sicherheitsrelevanten Vorgängen wie z. B. Veränderungen an der Infrastruktur, an den Plattformen und der Anwendungssoft-

ware, wie bestimmte Systemverwaltereingriffe, Änderung und Löschung von Anwendungsdaten, Logins und Programmaufrufe von Anwendern einer Protokollierung unterliegen. Entsprechende Anforderungen an Auditing- und Reportfunktionen sind in den SLAs festzulegen.

Protokolle bezüglich der Infrastruktursicherheit sind vom Anbieter zu führen und zu kontrollieren. Der Anwender sollte sich vertraglich vorbehalten, dass ihm Sicherheitsvorfälle, die seine Anwendungen betreffen können, rechtzeitig bekannt gemacht werden, damit er nötigenfalls eigene Konsequenzen ziehen kann. Seitens der Anwender sind die Aktivitäten an der Cloud-Schnittstelle einer Protokollierung zu unterwerfen, um fehlerhafte bzw. missbräuchliche Nutzungen des Cloud-Zugangs kontrollieren zu können.

5. Fazit

Cloud Computing steht für vielfältige Möglichkeiten, Dienstleistungen zur Datenverarbeitung unter Verwendung des Internet 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, PaaS 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 verhin-

dert 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 Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können;
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, 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;
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.