19. Wahlperiode

Drucksache **19/4762**

HESSISCHER LANDTAG

30. 03. 2017

Fünfundvierzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 2016
vom Hessischen Datenschutzbeauftragten
Prof. Dr. Michael Ronellenfitsch
nach § 30 des Hessischen Datenschutzgesetzes

Eingegangen am 30. März 2017 · Ausgegeben am 9. Mai 2017
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Fünfundvierzigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2016

gemäß § 30 des Hessischen Datenschutzgesetzes

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 45. Tätigkeitsbericht

2FA	2-Faktor-Authentifikation
a. a. O.	am angegebenen Ort
Abb.	Abbildung
ABDSG-E	Entwurf zum Allgemeinen Bundesdatenschutzgesetz
ABl.	Amtsblatt
Abs.	Absatz
ADV	Verträge über eine Datenverarbeitung im Auftrag
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
AOLG	Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden
Art.	Artikel
AVBWasserV	Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser
AWG	Außenwirtschaftsgesetz
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
bDSB	betriebliche Datenschutzbeauftragte
BDSG	Bundesdatenschutzgesetz
BFZ	Beratungs- und Förderzentren
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz)
BMG	Bundesmeldegesetz
BRDrucks.	Bundesratsdrucksache
BTDrucks.	Bundestagsdrucksache
BVerfGE	Bundesverfassungsgericht, Entscheidungssammlung
bzw.	beziehungsweise
ca.	cirka
CoC	Code of Conduct
d. h.	das heißt
DB	Deutsche Bahn AG
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSG-VO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DTAG	Deutsche Telekom AG
DuD	Datenschutz und Datensicherung (Zeitschrift)
e. V.	eingetragener Verein
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor (engl. Abkürzung für Europäischer Datenschutzbeauftragter)
EDSB	Europäischer Datenschutzbeauftragter
EG oder ErwG	Erwägungsgrund

EG	Europäische Gemeinschaft
EG-DR	EG-Datenschutzrichtlinie
EKD	Evangelische Kirche in Deutschland
EKG	Elektrokardiogramm
ENFAST	European Network of Fugitive Active Search Teams
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EU-US Privacy Shield	Durchführungsbeschluss der EU-Kommission über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes
FAZ	Frankfurter Allgemeine Zeitung
FDR	Falldatei Rauschgift
GbR	Gesellschaft bürgerlichen Rechts
GDPR	General Data Protection Regulation (engl. Abkürzung für DS-GVO)
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GewO	Gewerbeordnung
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GMK	Gesundheitsministerkonferenz
GPS	Global Positioning System, deutsch: Globales Positionsbestimmungssystem
grds.	grundsätzlich
GVBl.	Gesetz- und Verordnungsblatt für das Land Hessen
GVG	Gerichtsverfassungsgesetz
GWB	Gesetz gegen Wettbewerbsbeschränkungen
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HGB	Handelsgesetzbuch
HHG	Hessisches Hochschulgesetz
HIS	Hinweis- und Informationssystem
HKM	Hessisches Kultusministerium
HMDIS	Hessisches Ministerium des Innern und für Sport
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HWG	Hessisches Wassergesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. R.	in der Regel
i. S. d.	im Sinne der/des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
insb.	insbesondere
IVENA	Interdisziplinärer Versorgungsnachweis (webbasierte Anwendung, mit der sich die Träger der präklinischen und klinischen Patientenversorgung jederzeit in Echtzeit über die aktuellen Behandlungs- und Versorgungsmöglichkeiten der Krankenhäuser informieren können)
IT	Informationstechnik
JGG	Jugendgerichtsgesetz
JI-Richtlinie	Richtlinie des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
KIS	Krankenhausinformationssystem
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
KV Hessen	Kassenärztliche Vereinigung Hessen
KWG	Kreditwesengesetz
LTDrucks.	Landtagsdrucksache
LUSD	Lehrer- und Schülerdatenbank
m. E.	meines Erachtens
MDK	Medizinischer Dienst der Krankenversicherung
NFC	Near Field Communication
NIDA	Notfall-Informations- und Dokumentations-Assistent (digitales Verfahren für Einsatzprotokolle bei Rettungsleitstellen)
NRW	Nordrhein-Westfalen
o. a.	oben angegeben/angegebene/angegebener/angebenes
o. g.	oben genannt/genannte/genannter/genanntes
OH KIS	Orientierungshilfe Krankenhausinformationssysteme
OP	Operation
OSS	One-Stop-Shop
OWiG	Gesetz über Ordnungswidrigkeiten
PAD	Portable Application Description (standardisiertes, XML-basiertes Format für die Weitergabe und Publikation von Hersteller- und Programminformationen eines Softwareprodukts)
PC	Personal Computer
PIAV	Polizeilicher Informations- und Analyseverbund
PKI	Public Key Infrastructure
PSA	Privacy and Security Assessment
RBStV	Rundfunkbeitragsstaatsvertrag
Rdnr.	Randnummer
RDV	Recht der Datenverarbeitung (Zeitschrift)
RMV	Rhein-Main-Verkehrsverbund
S.	Seite *oder* Satz
s.	siehe
s. o.	siehe oben
s. u.	siehe unten
SGB	Sozialgesetzbuch
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz)
SIS II	Schengener Informationssystem II
sog.	sogenannte/sogenannter/sogenanntes

SSA	Staatliches Schulamt
StAnz.	Staatsanzeiger für das Land Hessen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SWR	Südwestrundfunk
TMG	Telemediengesetz
TOM(s)	technisch und organisatorische Maßnahmen
u. a.	unter anderem
u. Ä.	und Ähnliche/Ähnlicher/Ähnliches
u. U.	unter Umständen
UKGM	Universitätsklinikum Gießen und Marburg GmbH
USA	Vereinigte Staaten von Amerika
usw.	und so weiter
vgl.	vergleiche
vHGS	verbundweites Hintergrundsystem
VPN	Virtual Private Network
VU	Verkehrsunternehmen
VwGO	Verwaltungsgerichtsordnung
WHG	Wasserhaushaltsgesetz
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften

Gesetz/Vorschrift	**Fundstelle(n)**
AEUV	Vertrag über die Arbeitsweise der Europäischen Union i. d. F. vom 09.05.2008 (ABl. EG C 115 S. 47), zuletzt geändert durch die Akte vom 09.12.2011 (ABl. EU L 112 S. 21)
AO	Abgabenordnung i. d. F. vom 01.10.2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3234)
AVBWasserV	Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser i. d. F. vom 20.06.1980 (BGBl. I S. 750, 1067), zuletzt geändert durch Verordnung vom 11.12.2014 (BGBl. I S. 2010)
AWG	Außenwirtschaftsgesetz i. d. F. vom 06.06.2013 (BGBl. I S. 1482), zuletzt geändert durch Gesetz vom 03.12.2015 (BGBl. I S. 2178)
BDSG	Bundesdatenschutzgesetz i. d. F. vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 25.02.2015 (BGBl. I S. 162)
Beschluss 2007/533/JI	Beschluss des Rates vom 12.06.2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation SIS II (ABl. EU L 205 S. 63)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Gesetz vom 24.05.2016 (BGBl. I S. 1190)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) i. d. F. vom 07.07.1997 (BGBl. I S. 1650), zuletzt geändert durch Gesetz vom 26.07.2016 (BGBl. I S. 1818)
BMG	Bundesmeldegesetz vom 03.05.2013 (BGBl. I S. 1084), zuletzt geändert durch Gesetz vom 11.10.2016 (BGBl. I S. 2218)
DS-GVO	Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG Datenschutz-Grundverordnung (ABl. EU L 119 S. 1)
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche in der Fassung der Bekanntmachung vom 21.09.1994 (BGBl. I S. 2494; 1997 I S. 1061), zuletzt geändert durch Gesetz vom 08.07.2016 (BGBl. I S. 1594)
EG-Vertrag	Vertrag zur Gründung der Europäischen Gemeinschaft i. d. F. vom 02.10.1997, zuletzt geändert durch den Vertrag über den Beitritt der Republik Bulgarien und Rumäniens zur Europäischen Union vom 25.04.2005 (ABl. EG L 157 S. 11)
EU-US Privacy Shield	Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12.07.2016 gemäß Richtlinie 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes C(2016) 4176 (ABl. EU L 207 S. 1)
GDPR	General Data Protection Regulation (Englische Abkürzung für DS-GVO, Fundstelle siehe dort)
GewO	Gewerbeordnung i. d. F. vom 22.02.1999 (BGBl. I S. 202), zuletzt geändert durch Gesetz vom 11.11.2016 (BGBl. I S. 2500)

GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 23.12.2014 (BGBl. I S. 2438)
GVG	Gerichtsverfassungsgesetz i. d. F. vom 09.05.1975 (BGBl. I S. 1077), zuletzt geändert durch Gesetz vom 22.12.2016 (BGBl. I S. 3150)
GWB	Gesetz gegen Wettbewerbsbeschränkungen i. d. F. vom 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Gesetz vom 13.10.2016 (BGBl. I S. 2258)
HBeihVO	Hessische Beihilfenverordnung i. d. F. vom 05.12.2001 (GVBl. I S. 482, 491, 564), zuletzt geändert durch VO vom 28.09.2015 (GVBl I S. 370)
HBG	Hessisches Beamtengesetz vom 27.05.2013 (GVBl. I S. 218, 508, 578), zuletzt geändert durch Art. 2 des Gesetzes vom 05.02.2016 (GVBl. I S. 30)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 07.01.1999 (GVBl. I S. 98), zuletzt geändert durch Gesetz vom 14.07.2016 (GVBl. I S. 121)
HGB	Handelsgesetzbuch in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 05.07.2016 (BGBl. I S. 1578)
HHG	Hessisches Hochschulgesetz i. d. F. vom 14.12.2009 (GVBl. I S. 666), zuletzt geändert durch Gesetz vom 30.11.2015 (GVBl. I S. 510)
HSchG	Hessisches Schulgesetz i. d. F. vom 14.06.2005 (GVBl. I S. 441), zuletzt geändert durch Gesetz vom 24.03.2015 (GVBl. I S. 118)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14.01.2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 28.09.2015 (GVBl. I S. 346)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15.01.2010 (GVBl. I S. 18), zuletzt geändert durch Gesetz vom 26.06.2015 (GVBl. I S. 254)
HWG	Hessisches Wassergesetz i. d. F. vom 14.12.2010 (GVBl. I S. 548), zuletzt geändert durch Gesetz vom 28.09.2015 (GVBl. I S. 338)
JGG	Jugendgerichtsgesetz i. d. F. vom 11.12.1974 (BGBl. I S. 3427), zuletzt geändert durch Gesetz vom 17.07.2015 (BGBl. I S. 1332)
JI-Richtlinie	Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EG L 119 S: 89)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie i. d. Ausfertigung vom 09.01.1907 (BGBl. III Gliederungsnummer 440-3), zuletzt geändert durch Gesetz vom 16.02.2001 (BGBl. I S. 266)
KWG	Kreditwesengesetz i. d. F. vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3171)
OWiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 21.10.2016 (BGBl. I S. 2372)
RBStV	Gesetz zu dem Neunzehnten Rundfunkänderungsstaatsvertrag und zur Änderung des Gesetzes zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 27.06.2016 (GVBl. I S. 94)
SGBII	Sozialgesetzbuch Zweites Buch – Grundsicherung für Arbeitsuchende – i. d. F. vom 13.05.2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 31.07.2016 (BGBl. I S. 1939)
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung – vom 20.12.1988 (BGBl. I S. 2477), geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3234)
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – i. d. F. vom 11.09.2012 (BGBl. I S. 2022), zuletzt geändert durch Gesetz vom 11.10.2016 (BGBl. I S. 2226).
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz – i. d. F. vom 18.01.2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3234)
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz) i. d. F. vom 16.05.2001 (BGBl. I S. 876), zuletzt geändert durch Gesetz vom 18.07.2016 (BGBl. I S. 1666)
StGB	Strafgesetzbuch i. d. F. vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 22.12.2016 (BGBl. I S. 3150)
StPO	Strafprozessordnung i. d. F. vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 23.12.2016 (BGBl. I S. 3346)
TMG	Telemediengesetz i. d. F. vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 21.07.2016 (BGBl. I S. 1766)
VO EG 2580/2001	Verordnung (EG) Nr. 2580/2001 des Rates vom 27.12.2001 über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen zur Bekämpfung des Terrorismus (ABl. L 344/70)
VO EG 881/2002	Verordnung (EG) Nr. 881/2002 des Rates vom 27.05.2002 über die Anwendung bestimmter spezifischer restriktiver Maßnahmen gegen bestimmte Personen und Organisationen, die mit Osama bin Laden, dem Al-Qaida-Netzwerk und den Taliban in Verbindung stehen, und zur Aufhebung der Verordnung (EG) Nr. 467/2001 des Rates über das Verbot der Ausfuhr bestimmter Waren und Dienstleistungen nach Afghanistan, über die Ausweitung des Flugverbots und des Einfrierens von Geldern und anderen Finanzmitteln betreffend die Taliban von Afghanistan (ABl. L 139/9)
VO EU 753/2011	Verordnung (EU) Nr. 753/2011 des Rates vom 01.08.2011 über restriktive Maßnahmen gegen bestimmte Personen, Gruppen, Unternehmen und Einrichtungen angesichts der Lage in Afghanistan (ABl. L 199/1)
VwGO	Verwaltungsgerichtsordnung i. d. F. vom 19.03.1991 (BGBl. I S. 686), zuletzt geändert durch Gesetz vom 22.12.2016 (BGBl. I S. 3106) mit Wirkung vom 01.01.2017
WHG	Wasserhaushaltsgesetz i. d. F. vom 31.07.2009 (BGBl. I S. 2585), zuletzt geändert durch Gesetz vom 04.08.2016 (BGBl. I S. 1972)

Kernpunkte

1. Die Umsetzung der EU-Datenschutzreform nahm im Berichtsjahr Fahrt auf. Die neuen EU-Vorgaben wurden ausgewertet, erste Maßnahmen eingeleitet und Vorbereitungen getroffen. Die Auswirkungen, die auf Gesetzgeber, Datenschutzbehörden, Verwaltung, Wirtschaft und Unternehmen zukommen, können noch nicht abschließend überblickt werden. Es kann aber bereits jetzt festgestellt werden, dass die Datenschutzlandschaft sich nachhaltig verändern wird (Ziff. 1.2; 1.3; 2.4; 4.2.1; 4.3.1; 4.5.2; 8.4; 8.6; 9.; 10.3).

2. Trotz Kritik der Datenschutzbehörden verabschiedete die Europäische Kommission am 13.07.2016 in Aufarbeitung der Folgen des EuGH-Urteils vom 06.10.2015 zu Safe Harbor den EU-US-Privacy-Shield (Ziff. 2.3).

3. Videoüberwachung der Gefahrenabwehrbehörden kann unter Einhaltung datenschutzrechtlicher Vorgaben ein zulässiges und geeignetes Mittel zur Prävention sein. Im Berichtsjahr wurde ich von öffentlichen Stellen dahingehend um Beratung gebeten (Ziff. 5.2.2).

4. Zusammen mit der Bundesbeauftragten und einigen Landesdatenschutzbeauftragten habe ich die Verbunddatei „Rauschgift“ stichprobenartig überprüft. Die festgestellten Ergebnisse und Probleme (z. B. Speicherung von Bagatellfällen, Dokumentationen) flossen in einen gemeinsamen Prüfbericht und eine Entschließung der Datenschutzkonferenz ein (Ziff. 3.1.1; 8.7).

5. Das am 01.11.2015 in Kraft getretene Bundesmelderechtsgesetz löste die bisherigen Landesregelungen ab und führte in der Praxis zu Auslegungsfragen. Anhand einer Fallsammlung beantworte ich die häufigsten Fragestellungen (Ziff. 3.3.1).

6. Der Einsatz elektronischer Kommunikationsmittel (Handyfotos, gemeinsame Schulplattform) wirft im Schulbereich bei Eltern, Lehrern und Schulleitern kritische Fragestellungen auf (Ziff. 3.4.1; 3.4.3).

7. In Verwaltung und Wirtschaft führt die Entwicklung elektronischer Kommunikationswege wie Messenger-Dienste, E-Mail und Internet-Dienste zu Unsicherheiten im datenschutzgerechten Umgang (Ziff. 5.1.2; 4.8.1; 10.1; 5.1.1; 4.8.3).

8. Im Berichtsjahr habe ich verstärkt Außenprüfungen, zum Teil als Schwerpunktprüfungen, mit sehr unterschiedlichen Ergebnissen durchgeführt. Während bei Banken und Sparkassen ein hohes Datenschutzniveau festgestellt werden konnte, wurden bei zwei Wirtschaftsunternehmen und einem Steuerberater beanstandungswürdige Umstände vorgefunden (Ziff. 4.3.2; 4.3.3; 4.6.3).

9. Betreiber von Webseiten müssen bei Einbindung von Drittanbieter-Diensten ihre datenschutzrechtliche Mitverantwortung erfüllen. Dazu gehören insbesondere der Hinweis auf die Datenverarbeitung durch eigene und fremde Dienste auf der Webseite sowie das Angebot einer Widerspruchsmöglichkeit gegen Tracking-Dienste (Ziff. 4.7.2).

10. Eine Bonitätsanfrage bei Auskunfteien durch einen Onlineshop zur Steuerung der Zahlartenauswahl ohne kreditorisches Risiko ist unzulässig (Ziff. 4.7.3).

11. Bei der jährlich stattfindenden, internationalen Datenschutzprüfung wurden diesmal Dienste und Geräte aus dem Internet der Dinge untersucht. Bei der Prüfung der hessischen Anbieter standen besonders Geräte im Vordergrund, die unter dem Schlagwort „Smart Home“ vertrieben werden (Ziff. 4.7.1).

12. Zwar besteht für den Einsatz von Funkwasserzählern durch Wasserversorgungsunternehmen eine Rechtsgrundlage. Aber auch die Ausgestaltung des Erhebungs- und Verarbeitungsverfahrens muss expliziten datenschutzrechtlichen Grundsätzen genügen (Ziff. 4.4.3).

13. Der Abgleich von Kundendaten mit Antiterrorlisten ist zulässig (Ziff. 4.4.2).

14. Die Datenverarbeitung des RMV entsprach den vertraglichen Vorgaben. Es ist möglich, das eTicket anonym zu nutzen. Durch die jetzt jedem Kunden offenstehende Möglichkeit, die Kontrolldatensätze auf der Chipkarte löschen zu lassen, werden seine Interessen noch besser berücksichtigt (Ziff. 4.4.4).

15. Im Gesundheitsbereich fallen immer wieder Datenschutzverstöße auf, die es Dritten ermöglichen, Einsicht in sensible Patientendaten zu nehmen (Ziff. 6.2; 6.3; 6.7).

1. Einführung

1.1

Allgemeines

1.1.1

Informationelle Selbstbestimmung

Der Datenschutz stand im Berichtszeitraum nicht im Fokus des öffentlichen Interesses. Schlagzeilen machten die Erdoğan-Satire von Jan Böhmermann, der Putschversuch in der Türkei, Brexit, die Flüchtlingssituation in Europa, die US-Präsidentschaftswahl und die – vorwiegend islamistischen –- Terroranschläge. Bei der Würdigung dieser Ereignisse spielt der Datenschutz mehr oder weniger am Rande eine Rolle. Seine Bedeutung wurde dabei jedoch häufig verkannt. So frischte man die Legende vom Datenschutz als Wettbewerbsnachteil für die deutsche Wirtschaft durch seine Qualifizierung als Digitalisierungsbremse auf. In Wirklichkeit erwies sich der deutsche Datenschutz im Welthandel als Wettbewerbsvorteil. Ferner wurden vermeintliche datenschutzrechtliche Restriktionen für Defizite bei der Bekämpfung von Terrorismus und Gewaltkriminalität verantwortlich gemacht. Soweit diese Restriktionen wirklich bestehen, war und ist der HDSB bereit, bei der Ausgestaltung von Abhilfemaßnahmen zu kooperieren. Etwaige Abstriche beim Datenschutz müssen dann aber real zu einer effektiven Verbesserung der Sicherheitslage führen und auf das absolut Notwendige beschränkt bleiben. Ohnehin besteht kein originärer Widerspruch zwischen den Belangen der öffentlichen Sicherheit und des Datenschutzes. Widersprüche lösen sich zumeist auf, wenn man das Fehlverständnis des Datenschutzes korrigiert. Das Fehlverständnis beruht nicht zuletzt auf dem Sprachgebrauch. Der Ausdruck „Datenschutz“ stellte ursprünglich nur den Versuch dar, das US-amerikanische „Right to Privacy“ ins Deutsche zu übersetzen. Das führte zu zwei Irrtümern: Der Ausdruck „Datenschutz“ erweckt zum einen den Eindruck, als seien alle Daten geschützt. Zweck des Datenschutzes ist jedoch nicht der Schutz von Daten schlechthin. Gegenstand des Datenschutzes sind nur Daten, die bestimmte Informationen enthalten, Dritten mitgeteilt werden und dadurch einen Kommunikationsprozess in Gang setzen, bei dem die Informationen elektronisch verarbeitet und mit Hilfe des Internets ausgetauscht werden. Dieser Informationsaustausch umfasst auch Daten über andere Personen. Die Möglichkeit, automatisiert Daten zu verarbeiten, impliziert die Möglichkeit, sich Informationen über dritte Personen zu verschaffen, die diese Daten nicht preisgeben wollen. Durch die Möglichkeiten der automatisierten Datenverarbeitung können Persönlichkeitsbilder (Profile) generiert werden, die mehr über eine Person aussagen als dieser von sich selbst bekannt ist. Das beeinträchtigt die autonome Lebensführung. Nur den daraus erwachsenden Personenschutz bezweckt der Datenschutz. Nicht die Daten als solche werden somit geschützt, sondern die hinter den Daten stehenden Personen. Zum anderen wird die Privatheit zu eng gesehen. „Privacy“ wurde als Recht verstanden, allein gelassen zu werden. Der moderne Datenschutz betrifft indessen umfassend die informationelle Selbstbestimmung (BVerfGE 65, 1; 78, 77, 84; 84, 192,194; 103, 21, 23; 113, 29, 46; 115, 166 ;115, 320, 341 f.; 117, 202; 118, 168; 120, 274, 312; 120, 378, 397 ff.; 129, 208; 130, 1;133, 277; 138, 33, 40 ff. Zur Entstehung des Begriffs Wilhelm Steinmüller, Das informationelle Selbstbestimmungsrecht – wie es entstand und was man daraus lernen kann, RDV 2007, 158 ff.; Hans Peter Bull, Informationelle Selbstbestimmung – Vision oder Illusion, 2009, S. 25 ff. Zur Weiterentwicklung Marion Albers, Informationelle Selbstbestimmung, Analyse und Neukonzeption des Rechts auf informationelle Selbstbestimmung, 2002). Geschützt wird nicht lediglich und nicht einmal primär die Privatsphäre vor invasiven Eingriffen. Geschützt wird der ungehinderte Informationsaustausch. Der heutige Mensch will informativ und kommunikativ mit anderen in Verbindung treten. Er will Informationen verbreiten und möglichst umfassend und korrekt über alles und jedes informiert werden, aber autonom bestimmen, welche ihn betreffende Informationen verarbeitet werden und in die Öffentlichkeit gelangen dürfen. Informationszugangsfreiheit und Datenschutz sind zwei Seiten der gleichen Medaille. Ein richtig verstandenes Datenschutzgesetz ist immer zugleich ein Informationsfreiheitsgesetz. Hinzu kommt die Datensicherheit, die noch am ehesten dem Datenschutz als solchem nahe kommt, aber ebenfalls einen personalen Schutzzweck verfolgt. Für die informationelle Selbstbestimmung ist die Sicherheit der Daten unverzichtbar. Datenschutz, Informationszugangsfreiheit und Informationssicherheit gehören nach alledem zusammen. Ihre Kombination generiert die individuelle Datenhoheit oder Datensouveränität. Der Staat hat die informationelle Selbstbestimmung nicht nur zu achten; er hat sie auch zu schützen. Diese Verpflichtung trifft alle Staatsorgane. Die Intensität des Schutzes hängt vom Grad der Gefährdung der informationellen Selbstbestimmung ab. Vor allem durch das Fortschreiten der Digitalisierung hat die Gefährdung eine Dimension erreicht, die Zweifel weckt, ob ein zureichender Schutz der informationellen Selbstbestimmung überhaupt noch gewährleistet werden kann.

1.1.2

Aktuelle Gefährdungen

Im Digitalisierungszeitalter ringt der Datenschutz um seine zeitgemäße Positionierung. Seit Erlass der ersten datenschutzrechtlichen Regelungen vor vier Jahrzehnten (Hessisches

Datenschutzgesetz vom 07.10.1970, GVBl. I S. 625) ist die Informationsgesellschaft, vorangetrieben durch das Internet, in einem nicht vorhersehbaren Ausmaß Realität geworden. Die in Exabyte gemessene Datenmenge, die im Internet verfügbar ist, sprengt alle bekannten Dimensionen. Zur Kennzeichnung der Lage dient das Schlagwort „Big Data“. Big Data steht für die Verknüpfung einer derartigen Vielzahl von Daten aus beliebigen Quellen, dass die Datenschutzprinzipien als Anachronismen erscheinen (in diesem Sinn Ole Schröder, in FAZ 40/17.2 1016. S. 16). Die Rede ist bereits von Post Privacy als Bezeichnung für eine Epoche ohne Privatsphäre, auf die man sich zwangsläufig einstellen müsse (vgl. Volker Boehme-Neßler, Das Ende der Anonymität Wie Big Data das Datenschutzrecht verändert, DuD 2016, 419 ff.; Karl- Heinz Ladeur, „Big Data“ im Gesundheitsrecht – Ende der „Datensparsamkeit“?, DuD 2016 ,360 ff.). Umgekehrt kann man argumentieren, dass Big Data durch die Verknüpfungsmöglichkeiten alle Daten zu personenbezogenen Daten mache, was zu einer immensen Ausdehnung des Datenschutzrechts führen müsste. Begrifflich unterliegt Big Data ständigem Wandel. Unter „Big Data“ werden die unterschiedlichsten Vorgänge und Erscheinungen gefasst, bei denen große Datenmengen verarbeitet werden, so die zunehmende Überwachung der Bevölkerung durch Geheimdienste auch in westlichen Staaten, die individuelle Profilbildung von Kunden durch Unternehmen, die Delokalisierung der Datenspeicherung durch Cloud Computing, die Veränderung von Produktionsprozessen als vierter Phase der industriellen Entwicklung (Industrie 4.0, Internet der Dinge) und dgl. Da es keinen einheitlichen Begriff von Big Data gibt, lassen sich pauschale Aussagen zu konkreten Gefährdungen der informationellen Selbstbestimmung und zu den jeweils gebotenen staatlichen Schutzmaßnahmen nicht treffen. Generell kann nur festgestellt werden, dass die Menschen durch ihre Daten immer kontrollierbarer werden und dass es eine staatliche Verpflichtung ist, den Kontrollverlust auch gegenüber Big Data in Schranken zu halten. Dies hat bei den einzelnen Anwendungsbereichen von Big Data problem- und organbezogen zu geschehen. Entsprechendes gilt für die „smarten“ Alltagsprodukte, über die ich schon mehrfach berichtet habe (vgl. hierzu zuletzt die Pressemitteilung zum 31. Wiesbadener Forum Datenschutz am 03.11.2016).

1.1.3
Gesetzgebung

Die umfangreiche datenschutzrechtliche Gesetzgebung im Berichtszeitraum stand im Zeichen der europäischen Datenschutzreform, auf deren Fortgang im vorliegenden Tätigkeitsbericht an verschiedenen Stellen eingegangen wird (vgl. insbesondere Ziff. 1.2 und 1.3 sowie 2.4; 4.2.1, 4.3.1 und 4.5.2). Auf europäischer Ebene fand die Reform mit dem Inkrafttreten der Datenschutz-Grundverordnung am 04.05.2016 ihren (vorläufigen) Abschluss. Die Umsetzung durch die nationalen Gesetzgeber lief im Berichtszeitraum dagegen gerade erst an. Die europäische Datenschutzreform verfolgt u. a. den Zweck, die aktuellen Gefährdungen der informationellen Selbstbestimmung im Griff zu behalten. Hierzu ist sie auf Ergänzung durch das mitgliedstaatliche Datenschutzrecht angewiesen und auch angelegt (zu skeptisch Alexander Roßnagel/Christian Geminn/Silke Jandt/Philipp Richter, Datenschutzrecht 2016 „Smart“ genug für die Zukunft?, 2016, S. 175 ff.). Im vorliegenden Zusammenhang genügt der Hinweis, dass die Big-Data-Probleme und die datenschutzrechtlichen Implikationen der „smarten“ Alltagsprodukte auf dem Boden der DS-GVO durchaus angegangen werden können.

1.1.4
Rechtsprechung

Sowohl der Europäische Gerichtshof wie auch das Bundesverfassungsgericht haben im Berichtszeitraum wesentlich zum Schutz der informationellen Selbstbestimmung beigetragen.

1.1.4.1
Europäischer Gerichtshof

Der EuGH führte 2016 seine Rechtsprechung zur Vorratsdatenspeicherung fort. Im Urteil Digital Rights Irland vom 08.04.2014 (Rs. C-293/12; C-294/12, DÖV 2014, 617) hatte die Große Kammer des EuGH die Richtlinie 2002/58/EG vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, ABl. L 201, S. 37) in der Fassung der Richtlinie 2009/136/EG vom 25.11.2009 (ABl.L 337, S. 11) für ungültig erklärt, da sie den Grundsatz der Verhältnismäßigkeit verletze. Das bedeutete jedoch kein absolutes Verdikt der Vorratsdatenspeicherung. Vielmehr ging der EuGH von der prinzipiellen Zulässigkeit der Vorratsdatenspeicherung aus. Durch die zweigliedrige Prüfung des Verhältnismäßigkeitsgrundsatzes, bei der Erforderlichkeit und Angemessenheit vermengt werden, entstand der Anschein, die konkret unangemessene Vorratsdatenspeicherung lasse die Erforderlichkeit der Vorratsdatenspeicherung generell entfallen. Eben dies hat der EuGH aber nicht entschieden. Nach deutscher Rechtstradition besteht der Grundsatz der Verhältnismäßigkeit aus drei Teilgeboten, nämlich dem Gebot der Geeignetheit, der Erforderlichkeit und der Angemessenheit. Eine unangemessene Maßnahme kann folglich durchaus noch erforderlich sein. Der Schluss von der Unangemessenheit der Vorratsdatenspeicherung auf ihre generelle Entbehrlichkeit war somit verfehlt. In bestimmten Konstellationen konnte nach dem EuGH die erforderliche Maßnahme auch angemessen sein. Die nationalen Gesetzgeber sahen sich daher aufgerufen, solche Konstellationen zu umschreiben. Die diesbezügliche schwedische und britische Regelung wurden erneut dem EuGH vorgelegt. Am 21.12.2016 erging das Urteil in den verbundenen Rechtssachen C-203/15, Tele2 Sverige AB/Post-och telestyrelsen, und C-698/15, Secretary of State for the Home Department/Tom Watson u. a. Wiederum erklärte der EuGH die Vorratsdatenspeicherung grundsätzlich für zulässig, legte aber hierfür enge Schranken an. Danach dürfen die Mitgliedstaaten den Betreibern elektronischer Kommunikationsdienste keine allgemeine Verpflichtung zur Vorratsdatenspeicherung auferlegen. Das Unionsrecht untersage eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten. Es stehe den Mitgliedstaaten aber frei, vorbeugend eine gezielte Vorratsspeicherung dieser Daten zum alleinigen Zweck der Bekämpfung schwerer Straftaten vorzusehen, sofern eine solche Speicherung hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Speicherung auf das absolut Notwendige beschränkt sei. Der Zugang der nationalen Behörden zu den auf Vorrat gespeicherten Daten müsse von bestimmten Voraussetzungen, insbesondere einer vorherigen Kontrolle durch eine unabhängige Stelle und der Vorratsspeicherung der Daten im Gebiet der Union, abhängig gemacht werden. Implizit ist in dieser Anforderung die Verpflichtung enthalten, die unabhängige Stelle mit den für eine effektive Kontrolle nötigen personellen und sächlichen Mitteln auszustatten. Die Kontrolle schließt den Big-Data-Aspekt ein.

1.1.4.2

Bundesverfassungsgericht

Mit Urteil vom 20.04.2016 (1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781) entschied das Bundesverfassungsgericht über die Verfassungsbeschwerden gegen Vorschriften des Bundeskriminalamtsgesetzes (BKAG) in der Fassung vom 31.12.2008 (BGBl. I S. 3083). Dabei beanstandete die Senatsmehrheit eine Reihe von Verstößen gegen den Grundsatz der Verhältnismäßigkeit, die auch bei Big Data relevant sein könnten. Im Einzelnen argumentiert das Bundesverfassungsgericht wie folgt: Das angegriffene Gesetz ermächtigte das Bundeskriminalamt im Rahmen der Gefahrenabwehr und Straftatenverhütung zur heimlichen Erhebung personenbezogener Daten und begründe Eingriffe in die Grundrechte der Unverletzlichkeit der Wohnung, des Telekommunikationsgeheimnisses, der informationellen Selbstbestimmung sowie in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Es sei Aufgabe des Gesetzgebers, einen Ausgleich zwischen der Schwere dieser Grundrechtseingriffe und der Pflicht des Staates zum Schutz der Bevölkerung zu schaffen. Die angegriffenen Befugnisse ermöglichten tiefgreifende Eingriffe in die Privatsphäre, im Einzelfall auch in private Rückzugsräume, deren Schutz für die Wahrung der Menschenwürde von besonderer Bedeutung sei. Das Gewicht wirksamer Aufklärungsmittel zur Abwehr von Gefahren für die demokratische und freiheitliche Ordnung und den Schutz der Grundrechte sei jedoch ebenfalls in Rechnung zu stellen. Die Sicherheit des Staates und die von ihm - unter Achtung von Würde und Eigenwert des Einzelnen - zu gewährleistende Sicherheit der Bevölkerung stünden insoweit mit anderen hochwertigen Verfassungsgütern im gleichen Rang. Die dem Bundeskriminalamt eingeräumten Befugnisse seien vom Grundsatz her nicht zu beanstanden. Wo sie jedoch tief in die Privatsphäre eingreifen, unterlägen sie als Ausfluss des Verhältnismäßigkeitsgrundsatzes übergreifenden Anforderungen an ihre Ausgestaltung. Insbesondere müssten die Eingriffsbefugnisse auf den Schutz gewichtiger Rechtsgüter begrenzt bleiben und sich auf solche Fälle beschränken, in denen eine Gefährdung dieser Rechtsgüter hinreichend konkret absehbar sei. Auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson dürften sie sich nur unter eingeschränkten Bedingungen erstrecken. Für Befugnisse, die typischerweise mit einem Eindringen in den Kernbereich privater Lebensgestaltung verbunden seien, bedürfe es besonderer Schutzregelungen. Nötig sei ein hinreichender Schutz von Berufsgeheimnisträgern. Überdies bestünden verfassungsrechtliche Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Hierzu gehörten Benachrichtigungspflichten an die Betroffenen nach Durchführung der Maßnahmen, richterliche Kontrollbefugnisse, eine regelmäßige aufsichtliche Kontrolle sowie Berichtspflichten gegenüber Parlament und Öffentlichkeit. Schließlich müssten die Befugnisse mit Löschungspflichten flankiert sein. Diesen Anforderungen genügen nach Ansicht der Senatsmehrheit die angegriffenen Vorschriften in verschiedener Hinsicht nicht. Nicht hinreichend begrenzt sei die Regelung zum Einsatz von besonderen Mitteln zur Überwachung außerhalb von Wohnungen. Die Erstreckung der Telekommunikationsüberwachung auf die Straftatenverhütung und die Regelung zur Erhebung von Telekommunikationsverkehrsdaten seien zu unbestimmt und unverhältnismäßig weit. Allen angegriffenen Ermittlungs- und Überwachungsbefugnissen fehlten flankierende Regelungen. Die Unterscheidung zwischen Strafverteidigern und anderen Rechtsanwälten sei nicht tragfähig. Es fehle an hinreichenden Vorgaben zu turnusmäßigen Pflichtkontrollen, an einer umfassenden Protokollierungspflicht sowie an

Berichtspflichten gegenüber Parlament und Öffentlichkeit. Verfassungswidrig sei die Möglichkeit, von der Löschung erhobener Daten nach Zweckerfüllung allgemein abzusehen, soweit die Daten zur Verfolgung von Straftaten oder zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich seien. Für eine über das ursprüngliche Ermittlungsverfahren hinausreichende Verwendung der Daten seien die Grundsätze der Zweckbindung und Zweckänderung maßgeblich. Zu unterscheiden sei zwischen einer grundsätzlich zulässigen weiteren Nutzung der Daten im Rahmen des ursprünglichen Erhebungszweckes und einer Zweckänderung, die nur in bestimmten Grenzen erlaubt werden dürfe. Der Gesetzgeber könne eine Nutzung der Daten über das ursprüngliche Ermittlungsverfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung), solange die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaube. Darüber hinaus könne der Gesetzgeber eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung). Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientierten sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Diesen Grundsätzen genügen die Regelungen zur Nutzung und Übermittlung der Daten an inländische Behörden nur teilweise. Grundsätzliche Aussagen enthält die Entscheidung zu den Anforderungen an eine Übermittlung von Daten an ausländische Sicherheitsbehörden. Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürften durch einen Austausch zwischen den Sicherheitsbehörden nicht in ihrer Substanz unterlaufen werden. Der Gesetzgeber habe dafür Sorge zu tragen, dass dieser Grundrechtsschutz durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen ebenso wenig ausgehöhlt werde wie durch eine Entgegennahme und Verwertung von durch ausländische Behörden menschenrechtswidrig erlangten Daten. Durch diese Entscheidung hat das Bundesverfassungsgericht dem Gesetzgeber so detaillierte Vorgaben auferlegt, dass die Gesetzgebung fast schon Vollzugscharakter annimmt. An den Vorgaben sind künftige gesetzgeberische Aktionen zu messen (vgl. BVerfG, Beschluss vom 15.06.2016 – 1 BvR 2544/08), auch solche, die Big Data betreffen.

1.1.5

Verwaltung

Die Datenschutzaufsicht durch den HDSB ist funktionell der Exekutive zugeordnet. Sie erstreckt sich auch auf Big Data und wird insoweit von den statistischen Gesamtangaben unter Ziff. 1.4 miterfasst.

1.2

Datenschutzreform

Mit der Verabschiedung des europäischen Datenschutzpakets ist nach häufig kolportierter Auffassung eine neue Zeitrechnung im Datenschutzrecht angebrochen (vgl. Peter Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841 ff.). Big-Bang-Vorstellungen wären aber falsch. Das Reformpaket, dessen Entwicklung im Berichtszeitraum in der Folge dargestellt wird, hat vielmehr Kompromisscharakter, und ein Teil des Kompromisses besteht darin, dass die Umstellung des nationalen Rechts auf das Unionsrecht schrittweise erfolgt und die nationalen Gesetzgeber auch sonst gefordert sind.

1.2.1

Fortentwicklung des Unionsrechts

Die Trilogparteien, d. h. die Europäische Kommission, das Europäische Parlament und der Rat der Europäischen Union, haben sich am 16.12.2015 auf einen Text für die Neuregelung des Datenschutzes geeinigt. Die Neuregelung umfasst zum einen die Datenschutz-Grundverordnung, die die Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich abdeckt. Zum anderen haben sich die Trilogparteien auf eine Richtlinie speziell für die Datenverarbeitung im Polizei- und Justizbereich verständigt. Mit dem Gesetzgebungspaket werden die Vorschriften der Datenschutzrichtlinie von 1995 und des Rahmenbeschlusses von 2008 über den Schutz personenbezogener Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aktualisiert. Der Beitrag zeigt die wesentlichen Entwicklungen für beide Bereiche im Berichtszeitraum auf.

1.2.1.1
Datenschutz-Grundverordnung

Am 25.01.2012 hat die Europäische Kommission den Entwurf einer „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr“ vorgelegt [KOM (2012) 11: Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)]. Im Rahmen der ersten Lesung hat das Europäische Parlament zu diesem Vorschlag am 12.03.2014 Stellung genommen und Änderungsvorschläge beschlossen (44. Tätigkeitsbericht, Ziff. 1.2.1). Der Rat der Europäischen Union (Ministerrat) hat seine Beratungen bereits im Januar 2012 aufgenommen, seinen Standpunkt jedoch erst bei seinem Treffen am 15.06.2015 festgelegt (Rats-Dokument 9565/15). Die Beratungen im Rat erwiesen sich als schwierig, da die unterschiedlichen Rechtsordnungen der Mitgliedstaaten in Einklang gebracht werden mussten. Nachdem die Stellungnahmen von Rat und Parlament zu dem Verordnungsvorschlag vorlagen, konnten am 24.06.2015 die so genannten Trilog-Verhandlungen, d. h. die „Dreier-Gespräche“ zwischen Parlament, Ministerrat und Kommission, beginnen. Eine endgültige Einigung zu dem gesamten Reformpaket, bestehend aus Verordnung und Richtlinie, erfolgte am 16.12.2015. Am 04.05.2016 wurde der Text der Datenschutz-Grundverordnung im Amtsblatt veröffentlicht (ABl. L119, S. 1), am 25.05.2016 trat sie in Kraft. Die Datenschutz-Grundverordnung wird ab dem 25.05.2018 direkt in allen Mitgliedstaaten gelten. Sie regelt die Rechte natürlicher Personen sowie die Pflichten derjenigen, die die Daten verarbeiten bzw. für die Verarbeitung der Daten verantwortlich sind. Wesentliche Neuerungen gibt es dabei beispielsweise im Bereich der Sanktionen, wo nunmehr ein Bußgeld in Höhe von bis zu 4 % der Jahresumsätze des Unternehmens verhängt werden kann, sowie durch Einführung des so genannten Marktortprinzips. Dadurch sind auch Unternehmen an das europäische Datenschutzrecht gebunden, die nur ihre Dienste in Europa anbieten, selbst aber im Ausland ansässig sind. Auch die Nutzerrechte werden gestärkt: So ist zukünftig der Zugang zu den eigenen Daten erleichtert und das Recht auf Datenportabilität, also das Recht, die eigenen Daten von einem Dienst zu einem anderen zu übertragen, gewährleistet. Gestärkt wird außerdem das Recht des Nutzers auf „Vergessen werden“, d. h. auf Löschung der Daten unter bestimmten Voraussetzungen. Zum Vorteil der Unternehmen und natürlichen Personen wurde der so genannte One-Stop-Shop eingeführt, wodurch die Datenschutzbehörde des jeweiligen Mitgliedstaats, in dem das Unternehmen seine Hauptniederlassung hat bzw. in dem die Person wohnt, als Ansprechpartner für alle datenschutzrelevanten Fragen zur Verfügung steht.

1.2.1.2
JI-Richtlinie

Nachdem das Europäische Parlament seine Stellungnahmen zu Verordnungs- und Richtlinien-Vorschlag im März 2014 abgeben konnte, benötigte der Rat für seinen Standpunkt zur Richtlinie deutlich länger. Am 09.10.2015 hat er seine allgemeine Ausrichtung zum Richtlinien-Vorschlag der Kommission angenommen (Rats-Dokument 12555/15), unmittelbar im Anschluss konnten die Trilog-Verhandlungen beginnen. Die Kommission konnte mit der Gesamteinigung über Verordnungs- und Richtlinien-Vorschlag am 16.12.2015 wie gewünscht an der „Paketlösung“ festhalten. Am 04.05.2016 wurde auch der Text der Richtlinie im Amtsblatt der Europäischen Union veröffentlicht (ABl. L119, S. 89), einen Tag später trat die Richtlinie in Kraft. Diejenigen Vorschriften, die die Mitgliedstaaten in Umsetzung der Richtlinie im Polizei- und Justizbereich erlassen, sind ab dem 06.05.2018 anzuwenden. Die Richtlinie zielt darauf ab, das Recht des Einzelnen auf Schutz seiner personenbezogenen Daten zu wahren und gleichzeitig ein hohes Maß an öffentlicher Sicherheit zu garantieren. Sie gilt sowohl für die grenzüberschreitende als auch für die nationale Verarbeitung von Daten durch die zuständigen Behörden der Mitgliedstaaten zum Zwecke der Strafverfolgung.

1.2.2
Anpassung des nationalen Datenschutzrechts

Das europäische Reformpaket bedarf der Ergänzung und Umsetzung in nationales Recht. Hierfür bestehen weitere Gestaltungsspielräume des Bundes- und Landesgesetzgebers, als gemeinhin angenommen wird.

1.2.2.1
Anwendungsausschluss und Öffnungsklauseln

Das Datenschutzrecht ist komplex und schwer überschaubar. Als Idealvorstellung für die Anwendung von Datenschutzrecht wird demgegenüber die abschließende Regelung aller möglichen Fallkonstellationen in einem einzigen Gesetz propagiert. In hierarchisch-vertikal gegliederten Staaten schneidet sich diese Vorstellung mit dem Konzept der

Vollharmonisierung. Bereits die RL 95/46/EG wurde im Sinne einer Vollharmonisierung ausgelegt. Erst recht strebt die Datenschutzreform 2018 eine Vollharmonisierung an. Dabei ist zu berücksichtigen, dass nach ständiger Rechtsprechung des EuGH Begriffe einer Bestimmung des Unionsrechts, die für die Ermittlung ihres Sinns und ihrer Bedeutung nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten müssen (EuGH-Urteil vom 18.10.2016 – Rs-C135/15 – Griechenland/Nikoforidis, NJW 2017, 141 Rdnr. 28). Die Vorstellung, es seien künftig in der EU für die Beurteilung datenschutzrelevanter Rechtsfragen nur noch die DS-GVO und JI-RL heranzuziehen, wäre aber illusorisch. Spezielleres bereichsspezifisches Datenschutzrecht auf unionsrechtlicher Grundlage geht dem allgemeinen Datenschutzrecht vor. Das gilt für alle spezielleren Normierungen, die datenschutzrechtliche Bezüge in Gestalt einer Tatbestandskongruenz aufweisen. Das allgemeine Datenschutzrecht der EU verdrängt bei Tatbestandskongruenz allerdings auch das bereichsspezifische mitgliedstaatliche Datenschutzrecht. Das allgemeine Datenschutzrecht der EU enthält jedoch zahlreiche Öffnungsklauseln für bereichsspezifisches Datenschutzrecht der Mitgliedstaaten. Das Konzept der Vollharmonisierung ist schon insoweit aufgehoben. Zudem scheitert die Vollharmonisierung an der fehlenden, alle Datenschutzaspekte umfassenden Gesetzgebungskompetenz der EU. Die Gesetzgebungskompetenz der EU kann sich allein aus vertraglichem Primärrecht ergeben. Nach Art. 4 Abs. 1 EUV verbleiben alle der EU nicht in den Verträgen ausdrücklich übertragenen Zuständigkeiten bei den Mitgliedstaaten. Aus der vertraglichen Rückbindung der Unionskompetenzen folgt zwingend der Grundsatz der begrenzten Einzelermächtigung (Art. 5 Abs. 1 S. 1, Abs. 2 EUV). Die materiellrechtliche Einzelermächtigung für die DGV findet sich in Art. 16 AEUV. Sie umfasst lediglich den Tätigkeitsbereich von EU-Organen und den freien Datenverkehr. Ob der Justizbereich und der Bereich der öffentlichen Sicherheit wie generell der Hoheitsbereich der Mitgliedstaaten in die Regelungskompetenz des europäischen Verordnungsgebers fallen, ist zweifelhaft. Die Datenschutz-Grundverordnung trägt den Zweifeln partiell Rechnung, indem sie ihren Anwendungsbereich begrenzt und eine Vielzahl von Öffnungsklauseln enthält. Der Anwendungsausschluss erklärt die Verordnung nicht aus sich selbst heraus für unanwendbar, sondern stellt nur klar, worauf sich die Verordnung nicht erstreckt. Die Öffnungsklauseln gehen demgegenüber von einer bestehenden Gesetzgebungszuständigkeit der EU aus und billigen bzw. weisen dem mitgliedstaatlichen Gesetzgeber Ergänzungs- und Konkretisierungsaufgaben und -befugnisse zu. Bei der Übernahme des europäischen Reformpakets in nationales Recht sind somit originäre Gesetzgebungskompetenzen der Mitgliedstaaten von aus dem Unionsrecht abgeleiteten Regelungsgeboten und Regelungsoptionen zu unterscheiden. In diesem Rahmen können und müssen die Mitgliedstaaten für die Datenverarbeitung im öffentlichen und privaten Bereich auch weiterhin nationale Regelungen erlassen.

1.2.2.2
Bund

Im Bundesministerium des Innern wurde der Referentenentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU)2016/680 (DS-RL) Datenschutz-Grundverordnung erstellt, der am 23.11.2016 den Verbänden zur Stellungnahme vorgelegt wurde (vgl. https://www.gdd.de/downloads/aktuelles/Stellungnahmen/2%/Entwurf.Stand 23.11.2016_DSnpUG-EU.pdf). Zentrales Element des Entwurfs ist die Neufassung des Bundesdatenschutzgesetzes. Kritische Äußerungen zum Entwurf, die von mir mitgetragen werden, finden sich unter Ziff. 10.3.

1.2.2.3
Hessen

Auf Landesebene befindet sich eine Anpassung des Hessischen Datenschutzgesetzes an die Vorgaben des Unionsrechts in Vorbereitung. In die Beratungen bin ich eingebunden.

1.3
DS-GVO:
Neue Bußgelder im Datenschutz

Die europäische Datenschutzreform verfolgt mit der DS-GVO unter anderem auch eine konsequentere Durchsetzung der Vorschriften der Verordnung (EG 148). Eine Maßnahme im Rahmen der Abhilfebefugnisse gemäß Art. 58 Abs. 2 DS-GVO ist nach Art. 58 Abs. 2 lit. i) DSG-VO die Verhängung von Geldbußen gemäß Art. 83 DS-GVO. Der Bußgeldrahmen wurde für die administrative Sanktion gegen Unternehmen erheblich erhöht.

Mit der europäischen Datenschutzreform hat die Sanktionierung von Datenschutzverstößen eine neue Qualität erlangt. Die nach der Datenschutz-Grundverordnung verhängbaren

Bußgelder lassen das Thema Datenschutz im Compliance-Ranking der Unternehmen deutlich nach oben klettern.

1.3.1

Ausgangslage in Deutschland

In Deutschland hat die „administrative Sanktion“ Tradition. Man unterscheidet zwischen dem Kriminal- und dem Ordnungsunrecht. Letzteres zeichnet sich dadurch aus, dass es mit einer Geldbuße geahndet wird. Im deutschen Ordnungswidrigkeitenverfahren gilt entgegen dem Strafrecht nicht der Legalitätsgrundsatz, der die Verfolgung der Tat stets verlangt, sondern der Opportunitätsgrundsatz, d. h. die Verfolgungsbehörde entscheidet nach pflichtgemäßem Ermessen (§ 47 OWiG), ob sie die Ordnungswidrigkeit verfolgt.

Die Geldbuße ist in erster Linie darauf gerichtet, eine bestimmte Ordnung durchzusetzen. Sie ist ein, mit einer Sanktion verbundener, spürbarer Pflichtenappell an den Betroffenen sich in Zukunft an diese Ordnung zu halten, sich nach dieser Ordnung zu richten. Die Geldbuße ist eine Pflichtenmahnung, die keine ins Gewicht fallende Beeinträchtigung des Ansehens und des Leumunds des Betroffenen zur Folge hat (BVerfGE 27, 18, 33).

Die Bußgeldtatbestände für Datenschutzverstöße sind derzeit in § 43 Abs. 1 und 2 BDSG geregelt. § 43 Abs. 1 BDSG listet Tatbestände auf, bei denen gemäß § 43 Abs. 3 S. 1, 1. Halbsatz BDSG ein Bußgeld bis zu 50.000 EUR verhängt werden kann. In § 43 Abs. 2 BDSG werden schwere Verstöße aufgeführt, für die gemäß § 43 Abs. 3 S. 1, 2. Halbsatz BDSG ein Bußgeld bis zu 300.000 EUR verhängt werden kann.

Das geltende Verfahren kann geführt werden gegen

- natürliche Personen,
- natürliche und juristische Personen im gemeinsamen Verfahren,
- eine natürliche Person und die juristische Person als Nebenbeteiligte in getrennten Verfahren.

Die Durchführung des Ordnungswidrigkeitenverfahrens richtet sich nach dem OWiG und über § 46 Abs. 1 OWiG nach den damit in Zusammenhang stehenden Gesetzen (StPO, GVG und JGG).

1.3.2

Die neuen Regelungen nach der DS-GVO

Ab dem 25.05.2018 wird für die Unternehmen mit der Datenschutz-Grundverordnung in Sachen Bußgelder wegen Verstöße gegen diese Verordnung eine „steife Brise“ wehen. Der Kanon der Bußgeldtatbestände wurde erheblich erweitert und der Bußgeldrahmen exorbitant erhöht. Die Geldbuße nach der DS-GVO hat in den Fällen des Art. 83 Abs. 5 und 6 DS-GVO wirksam, verhältnismäßig und abschreckend zu sein. Damit kann ein Bußgeld wegen eines Datenschutzverstoßes gegen ein Unternehmen diesem richtig „wehtun“. Es wird nicht zum Mast- und Schotbruch oder gar zum Untergang reichen, aber ein kurzzeitiger Starkwind wird nicht auszuschließen sein.

Die Regelung in Art. 83 DS-GVO trifft auf unterschiedliche Rechtstraditionen in den Mitgliedstaaten. Diese berücksichtigt die DS-GVO. In Art. 83 Abs. 9 DS-GVO heißt es beispielsweise:

> Art. 83 Abs. 9 DS-GVO
>
> Sieht die Rechtsordnung eines Mitgliedstaates keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen haben. In jedem Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen haben, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

In Erwägungsgrund 151 wird erläutert:

> EG 151
>
> Nach den Rechtsordnungen Dänemarks und Estlands sind die in dieser Verordnung vorgesehenen Geldbußen nicht zulässig. Die Vorschriften über Geldbußen können so angewandt werden, dass die Geldbuße in Dänemark durch die zuständigen nationalen Gerichte als Strafe und in Estland durch die Aufsichtsbehörden im Rahmen eines Verfahrens bei Vergehen verhängt wird, sofern eine solche Anwendung der Vorschriften in diesen

Mitgliedstaaten die gleiche Wirkung wie die von den Aufsichtsbehörden verhängten Geldbußen hat. Daher sollten die zuständigen nationalen Gerichte die Empfehlung der Aufsichtsbehörde, die die Geldbuße in die Wege geleitet hat, berücksichtigen. In jedem Fall sollten die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein.

Es obliegt den einzelnen Mitgliedstaaten das Verfahrensrecht zum Bußgeldverfahren zu regeln. Die Grundverordnung gibt hierfür in Erwägungsgrund 148 vor, dass es für die Verhängung von Geldbußen angemessene Verfahrensgarantien geben sollte, die den allgemeinen Grundsätzen des Unionsrecht und der Charta einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren entsprechen. Inwieweit die verschiedenen Ansätze der Mitgliedstaaten über Art. 83, Art. 70 Abs. 1 lit. k) DS-GVO harmonisiert werden können, bleibt abzuwarten.

1.3.3
Die Zuständigkeit

Der HDSB wird weiterhin zuständige Verfolgungsbehörde sein. Die Aufsichtsbehörde ist nach Art. 55 Abs. 1 DS-GVO für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet des eigenen Mitgliedstaats zuständig.

Im Zusammenhang mit dem Bußgeldverfahren ergeben sich daraus folgende Aufgaben:
- Durchsetzung der Verordnung (Art. 57 Abs. 1 lit. a) DS-GVO)
- Interne Verzeichnisse über Verstöße gegen diese Verordnung und gemäß Art. 58 Abs. 2 DS-GVO ergriffene Maßnahmen führen
- Im Rahmen der Befugnisse gemäß Art. 58 hat die Aufsichtsbehörde Untersuchungsbefugnisse (Art. 58 Abs. 1 DS-GVO) und
- Abhilfebefugnisse (Art. 58 Abs. 2 DS-GVO).

Ein Tätigwerden der Aufsicht im Rahmen des Bußgeldverfahrens schließt weitere Maßnahmen im Rahmen der Abhilfebefugnis aus Art. 58 Abs. 2 DS-GVO nicht aus.

In Erwägungsgrund 148 heißt es hierzu:

EG 148

Im Interesse einer konsequenteren Durchsetzung der Vorschriften dieser Verordnung sollten bei Verstößen gegen diese Verordnung zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß dieser Verordnung verhängt, oder an Stelle solcher Maßnahmen Sanktionen einschließlich Geldbußen verhängt werden. Im Falle eines geringfügigen Verstoßes oder falls voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden.

Die Aufsichtsbehörde hat durch die Grundverordnung bereits einen Strauß an Maßnahmen an die Hand gegeben bekommen. Gemäß Art. 58 Abs. 6 DS-GVO kann darüber hinaus jeder Mitgliedstaat außerdem durch Rechtsvorschriften vorsehen, dass seine Aufsichtsbehörde neben den in den Absätzen 1, 2, 3 aufgeführten Befugnissen über zusätzliche Befugnisse verfügt, sofern die Ausübung dieser Befugnisse die effektive Durchführung des Kapitels VII der DS-GVO nicht beeinträchtigt. Der Bundes- und die Landesgesetzgeber haben nun bis Mai 2018 Zeit, die Öffnungsklausel auszukleiden.

1.3.4
Die Tatbestände

Die Bußgeldtatbestände der DS-GVO sind in Art. 83 Abs. 4, 5, 6 DS-GVO geregelt. Die Datenschutzverstöße teilen sich in zwei Gruppen auf:

Gruppe 1
Tatbestände gemäß Art. 83 Abs. 4 DS-GVO
Bußgelder bis zu 10 Mio. EUR bzw. 2 % des weltweit erzielten Jahresumsatzes

Gruppe 2
Tatbestände gemäß Art. 83 Abs. 5 und 6 DS-GVO
Bußgelder bis zu 20 Mio. EUR bzw. 4 % des weltweit erzielten Jahresumsatzes

Bei Verstößen gegen Tatbestände der zweiten Gruppe gemäß Art. 83 Abs. 5 und 6 DS-GVO sind in jedem Einzelfall Bußgelder zu verhängen, die wirksam, verhältnismäßig und abschreckend sind. Ob es ein Redaktionsversehen war, dass die Bußgeldtatbestände gemäß Art. 83 Abs. 4 DS-GVO nicht aufgelistet wurden, oder ob das gewollt war, ist noch abzuwarten. Für Verstöße der Gruppe 1 würden so derzeit weichere Maßstäbe gelten.

1.3.4.1
Bußgeldtatbestände der Gruppe 1 (Art. 83 Abs. 4 DS-GVO)

Nach Art. 83 Abs. 4 lit. a) DS-GVO können Verstöße gegen Pflichten der Verantwortlichen und Auftragsverarbeiter gemäß Art. 8, 11, 25 bis 39, 42 und 43 DS-GVO geahndet werden. Das sieht zunächst einmal nach einem überschaubaren Kanon an Tatbeständen aus. Aber wenn man sich die in Bezug genommenen Artikel genauer anschaut, hat es sich der Verordnungsgeber recht einfach gemacht. Die Artikel haben in ihrer Bestimmtheit sehr unterschiedliche Qualität. Während beispielsweise Art. 31, 35 DS-GVO dem Adressaten die Pflichten klar vorgeben, stochert man als Verantwortlicher oder Auftragsverarbeiter bei Art. 8, 25 und 29 DS-GVO eher im Nebel.

Verwirrung in der praktischen Anwendung dürfte auch der Bezug auf Art. 42, 43 in Art. 83 Abs. 4 lit. a) im Verhältnis zu Art. 83 Abs. 4b) stiften. Die hier getroffene Differenzierung wird auf den ersten Blick nicht deutlich. Die Unterscheidung liegt allein darin, dass nach
Abs. 4 lit. a) Verstöße gegen Pflichten der Verantwortlichen und Auftragsverarbeiter geahndet werden können.
Dahingegen werden nach Art. 83 Abs. 4 lit. b) Verstöße gegen Pflichten der Zertifizierungsstelle gemäß Art. 42 und 43 DS-GVO geahndet.

Art. 83 Abs. 4 lit. c) DS-GVO sanktioniert Verstöße gegen die Pflichten der Überwachungsstelle gemäß Art. 41 Abs. 4 DS-GVO betreffend die Überwachung der Einhaltung der Verhaltensregeln gemäß Art. 40 DS-GVO.

1.3.4.2
Bußgeldtatbestände der Gruppe 2 (Art. 83 Abs. 5 und 6 DS-GVO)

Geldbußen bis zu 20 Mio. EUR bzw. 4 % des weltweit erzielten Jahresumsatzes können bei folgenden Verstößen verhängt werden:

- Art. 83 Abs. 5 lit. a) DS-GVO:
  Verstöße gegen die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Art. 5, 6, 7 und 9 DS-GVO
- Art. 83 Abs. 5 lit. b) DS-GVO:
  Verstöße gegen die Rechte der betroffenen Personen gemäß den Art. 12 bis 22 DS-GVO
- Art. 83 Abs. 5 lit. c) DS-GVO:
  Verstöße gegen die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Art. 44 bis 49 DS-GVO
- Art. 83 Abs. 5 lit. d) DS-GVO:
  Verstöße gegen alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden
- Art. 83 Abs. 5 lit. e) DS-GVO:
  Nichtbefolgung einer Anweisung oder vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Art. 58 Abs. 2 DS-GVO oder Nichtgewährung des Zugangs unter Verstoß gegen Art. 58 Abs. 1 DS-GVO
- Art. 83 Abs. 6 DS-GVO:
  Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2 DS-GVO. Unklar bleibt im Zusammenhang mit Art. 83 Abs. 6 DS-GVO, in welchem Verhältnis er zu Art. 83 Abs. 5 lit. e) DS-GVO steht. Auch hier findet sich eine nicht nachvollziehbare Dopplung der Tatbestände.

Allen Tatbeständen in den Absätzen 4, 5 und 6 ist gemeinsam, dass sie getreu europäischer Rechtsetzung relativ unbestimmt sind. Es bleibt also abzuwarten, wie das mit der nationalen Rechtsprechung in Einklang zu bringen sein wird.

1.3.5
Der neue Bußgeldrahmen

Das Europäische Gemeinschaftsrecht kennt die Geldbuße vor allem als Sanktion für Zuwiderhandlungen auf dem Gebiet des Kartellrechts. Die „administrative sanction“ ist im Grunde mit der Geldbuße unseres Ordnungswidrigkeitenrechts vergleichbar. Die Europäisierung des deutschen Kartellrechts hat sich in den letzten 20 Jahren vollzogen. Es nimmt für die Europäisierung des Datenschutzrechts in Fragen der Sanktionierung sozusagen eine Vorbildfunktion ein. Die Vorbildfunktion bezieht sich auf die Höhe von Geldbußen, die Zumessung von Geldbußen und den Unternehmensbegriff, nämlich den funktionellen Unternehmensbegriff.

1.3.5.1
Umfang

Neu im Datenschutzrecht ist, dass die Bestimmung der Geldbuße der Höhe nach eine so zentrale Bedeutung einnimmt. Die DS-GVO setzt Obergrenzen, die einen weiten Spielraum eröffnen und zum anderen in schwindelerregende Höhen führen können.

Nach Art. 83 Abs. 4 DS-GVO können bis 10 Mio. EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem welcher Betrag höher ist.

Bei Verstößen gegen die Grundsätze der DS-GVO, gegen die Regelungen zur Rechtmäßigkeit der Datenverarbeitung oder die Rechte des Betroffenen (Art. 83 Abs. 5 DS-GVO) und bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2 DS-GVO (Art. 83 Abs. 6 DS-GVO) werden im Einklang mit Art. 83 Abs. 2 DS-GVO Bußgelder in einer Höhe bis zu 20 Mio. EUR oder im Fall eines Unternehmens von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres festgesetzt, je nachdem welcher Betrag höher ist.

1.3.5.2
Bußgeldzumessung

Nach Art. 83 Abs. 2 DS-GVO werden Geldbußen je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 lit. a) bis h) und i) DS-GVO verhängt. Hierzu sei angemerkt, dass vermutlich eigentlich der Bezug Art. 58 Abs. 2 lit. a) bis h) und j) DS-GVO gemeint ist, denn lit. i) bezieht sich auf die Geldbuße und das macht keinen Sinn, denn nach „h“ käme „i“ im Alphabet. Eine offizielle Korrektur seitens der EU liegt aber bislang noch nicht vor.

Ob ein Bußgeld verhängt wird oder nicht und wie hoch das Bußgeld im Falle des Falles ist, richtet sich nach dem Kriterienkatalog des Art. 83 Abs. 2 DS-GVO, den allgemeinen Maßgaben des Art. 83 Abs. 1 DS-GVO sowie den ggf. noch zu erstellenden Leitlinien i. S. d. Art. 70 Abs. 1 lit. k) DS-GVO.

Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gemäß Art. 83 Abs. 2 lit. a) bis k) gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Art. 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i) Einhaltung der nach Art. 58 Abs. 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j) Einhaltung von genehmigten Verhaltensregeln nach Art. 40 oder genehmigten Zertifizierungsverfahren nach Art. 42 und
k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

Dieser Katalog verschriftlicht im Grunde, was bereits Bußgeldpraxis ist. Ergänzt wird er durch weitere allgemeine Maßgaben der DS-GVO für die Bußgeldpraxis:

- bei geringfügigen Verstößen kann eine Verwarnung ausreichen, ohne dass ein Bußgeld verhängt wird (Erwägungsgrund 148 Satz 2 DS-GVO);
- wurde der Verstoß von einer natürlichen Person begangen, die durch ein Bußgeld in unverhältnismäßigem Maße belastet würde, kann eine Verwarnung ohne Bußgeld gleichfalls ausreichen (Erwägungsgrund 148 Satz 2 DS-GVO);

- wurde der Verstoß von einer natürlichen Person begangen, sind bei der Bemessung des Bußgelds die Vermögensverhältnisse der Person und die allgemeinen Einkommensverhältnisse in deren Heimatstaat zu berücksichtigen (Erwägungsgrund 150 Satz 4 DS-GVO).

Die Bußgeldzumessung wird darüber hinaus in Anlehnung an das Kartellrecht komplexer. Neu für das Ordnungswidrigkeitenverfahren sind bei Datenschutzverstößen die Leitlinien für die Zumessung von Bußgeldern. Im deutschen Datenschutzrecht gab es bislang keine Leitlinien. Die DS-GVO eröffnet dem Europäischen Datenschutzausschuss gemäß Art. 70 lit. k) DS-GVO, Leitlinien für die Aufsichtsbehörden für die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO auszuarbeiten.

Die Vorgaben in Art. 83 Abs. 2 DS-GVO sollen durch die noch zu verfassenden Leitlinien des EDPB (Art. 70 lit. k), 2. Halbsatz DS-GVO) ergänzt werden. Aktuell arbeitet die Art. 29-Gruppe an einem Vorschlag für Leitlinien zur Bußgeldzumessung, der dann nach Konstituierung des EDPB verabschiedet werden müsste. Ziel ist es, hierdurch die Bußgeldzumessung für Unternehmen transparenter zu gestalten. Mittels der Leitlinien nach Art. 70 Abs. 1 lit. k) sollen sanktionsmildernde und sanktionsverschärfende Faktoren festgelegt werden, die den Unternehmen Anhaltspunkte für ein gesetzeskonformes Verhalten geben können. Sofern diese Leitlinien die Verwaltung in ihrer Verwaltungspraxis binden, kann dies mit der Maßgabe der Betrachtung des Einzelfalls nicht ohne weiteres konform gehen. Ob diese Art der Zumessung zur gewünschten kohärenten Auslegung der Vorschriften führt, bleibt ebenfalls abzuwarten.

1.3.5.3
Funktionaler Unternehmensbegriff

Im Hinblick auf die Frage, auf welchen Teil des Unternehmens der weltweite Umsatz für die Bußgeldzumessung zu beziehen ist, wurde für den Datenschutz der funktionale Unternehmensbegriff aus dem europäischen Kartellrecht übernommen. Dies ergibt sich aus Erwägungsgrund 150 Satz 3.

> EG 150 Satz 3
>
> Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden.

Nach ständiger Rechtsprechung des EuGH geht Art. 101 und 102 AEUV von einem funktionalen Unternehmensbegriff aus. Der funktionale Unternehmensbegriff orientiert sich an der wirtschaftlichen Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierungen (ständige Rspr. des EuGH; z. B. EuGH, Slg. 1991, I-2010 Rdnr. 21; EuGH, Slg. 2006, I-6391, Rdnr. 25).

Die Anwendung des im europäischen Kartellrecht wurzelnden Unternehmensbegriffs hat unter anderem für die Höhe der zu verhängenden Bußgelder nach Art. 83 DS-GVO weitreichende Folgen. Begeht eine Unternehmenstochter einen durch Bußgeld zu ahndenden Verstoß gegen die DS-GVO und liegt eine wirtschaftliche Einheit in Bezug auf die Muttergesellschaft vor, so bildet der gesamte weltweite Konzernumsatz (Mutter plus Tochter) die Berechnungsgrundlage für die Höhe des Bußgeldes.

Da die bisherige Rechtsprechung sich dem funktionalen Unternehmensbegriff aus der Perspektive des Kartellrechts genähert hat und den Unternehmen diese Auslegung unter pekuniären Aspekten nicht munden wird, ist damit zu rechnen, dass diese Auslegung des Unternehmensbegriffs im Rahmen gerichtlicher Verfahren angegriffen werden wird. Der heutige wirtschaftliche Faktor der Daten als Ware rechtfertigt einen solchen Transfer aus dem Kartellrecht vollumfänglich.

1.3.6
DSAnpUG-EU (Stand: 23.11.2016, 09:18 Uhr)

Im Zweiten Entwurf des Nachfolgegesetzes zum BDSG werden in Teil 2 Kapitel 5, §§ 39 bis 42 Regelungen über Sanktionen getroffen. § 39 EU-DSAnpUG-EG regelt im Sinne von Art. 83 Abs. 8 DS-GVO die Anwendung der Vorschriften über das Bußgeld- und Strafverfahren. Über § 40 Abs. 2 EU-DSAnpUG-EG kann auch derjenige bebußt werden, der in Ausübung seiner Tätigkeit für den Verantwortlichen oder Auftragsdatenverarbeiter vorsätzlich oder fahrlässig einen der in Art. 83 Abs. 4 bis 6 DS-GVO genannten Verstöße begeht. Diese Ordnungswidrigkeit kann gemäß § 40 Abs. 1 EU-DSAnpUG-EG mit einer Geldbuße von bis zu 300.000 EUR sanktioniert werden.

Umstritten war im Vorfeld, ob es zu verantworten ist, dass die immens hohen Bußgelder vor Amtsgerichten verhandelt werden. Die Lösung ist nun, dass gemäß § 39 Abs. 2 DSAnpUG-

EG dann vor dem Landgericht verhandelt wird, wenn die Geldbuße einen Betrag von 5.000 EUR übersteigt.

Ein weiterer langgehegter Wunsch der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat sich in dem Entwurf des DSAnpUG-EG auch realisiert. Die Staatsanwaltschaft soll das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen können.

Das DSAnpUG-EG soll noch vor Ende der Wahlperiode des Bundestags verabschiedet werden. Im Zeitpunkt der Erstellung dieses Berichts ist der Gesetzesentwurf in der Länderbeteiligung.

1.3.7

Herausforderungen für den Stichtag 25.05.2018

Eine Herausforderung wird sein, die Bußgeldtatbestände, insbesondere die in Art. 83 Abs. 4 DS-GVO, zu verifizieren und herauszuarbeiten, welche Pflichten sich aus den Art. 8, 11, 25 bis 39, 42 und 43 DS-GVO ergeben. Wie Art. 83 Abs. 4 lit. a) von Absatz 4 lit. b) DS-GVO im Hinblick auf die Pflichten aus Art. 43 DS-GVO abzugrenzen ist. Oder wie Art. 83 Abs. 5 lit. e) von Art. 83 Abs. 6 DS-GVO abzugrenzen ist.

Die DS-GVO enthält viele unbestimmte Regelungen/Rechtsbegriffe, Klauseln, die zu füllen sind und derzeit zugegebenermaßen zu einer für Unternehmen nicht kalkulierbaren Rechtsunsicherheit führen. Hier ist zu erwarten, dass die Bußgeldverfahren in den ersten Jahren vermehrt einer gerichtlichen Überprüfung unterzogen werden.

1.4

Arbeitsstatistik 2016

Das Berichtsjahr war geprägt von intensiven Arbeiten zur Umsetzung der Datenschutz-Grundverordnung und der JI-Richtlinie.

Zunächst waren die beiden EU-Texte in aufwändiger Detailarbeit nach Änderungen, neuen Aufgaben und Aufträgen an die Datenschutzbehörden zu untersuchen. Die Ergebnisse waren auszuwerten und zu definieren. Dazu fanden u. a. zahlreiche Treffen der Datenschutzbeauftragten des Bundes und der Länder untereinander in verschiedenster Zusammensetzung statt, aber auch Treffen mit Vertretern der Gesetzgebung auf Bund- und Länderebene und mit Vertretern aus Parlament, Verbänden, Kammern und den Medien. Zudem wurden zahlreiche Informationsvorträge gehalten und die gesetzestechnische Umsetzung sowohl auf Bundes- als auch auf Landesebene von mir begleitet.

Diese zeitintensiven, oft mit mehrtägigen Dienstreisen verbundenen Aufgaben beschäftigten einen Großteil meiner Mitarbeiter und Mitarbeiterinnen zusätzlich zu dem alltäglichen operativen Geschäft. Abgeschlossen ist die Umsetzungsphase noch nicht. Sie wird meine Dienststelle – wie auch die übrigen Aufsichtsbehörden – auch noch über das nächste Jahr hinaus beschäftigen.

In der nachfolgenden Tabelle sind Angaben zur Anzahl der Eingaben und Beratungsanfragen dargestellt, die neben der Bearbeitung von Grundsatzfragen, Stellungnahmen zu Gesetzesvorhaben und der Marktbeobachtung im Bereich von IT-Produkten einen wesentlichen Teil meiner Tätigkeit ausmachen. Diese Statistik wird weitgehend automationsgestützt mit Hilfe des eingesetzten Dokumentenverwaltungssystems erstellt. Nicht erfasst werden die zahlreichen telefonisch eingegangenen und telefonisch erledigten Eingaben und Beratungen, die zwar keinen Niederschlag in Akten gefunden haben, aber oft einen erheblichen Zeitaufwand verursachen. Die telefonischen Eingaben und Beratungen wurden für den Monat November als Stichprobe gezählt und für das Jahr hochgerechnet. Die Summe der telefonischen Erledigungen fällt in diesem Berichtsjahr niedriger aus, da die Mitarbeiter und Mitarbeiterinnen aufgrund der durch die DS-GVO erforderlich gewordenen Abstimmungsprozesse erheblich häufiger dienstlich unterwegs waren als im Vorjahr.

Die Anzahl der schriftlich dokumentierten Beratungen und Eingaben blieb im Wesentlichen gleich, wobei der Schwerpunkt der Thematik sich auf den Bereich von „Miete, Wohnen, Nachbarschaft“ verlagerte, was allerdings auf die zahlreichen Eingaben zur Videobeobachtung durch Haus- und Wohnungseigentümer bzw. Nachbarn zurückgeht.

Arbeitsstatistik des Hessischen Datenschutzbeauftragten zu Eingaben und Beratungen

Fachgebiet	Anzahl
Wohnen, Miete, Nachbarschaft	315
Auskunfteien und Inkassounternehmen	237
Elektronische Kommunikation, Internet	167
Schulen, Hochschulen, Archive	137
Kommunen	135

Gesundheit, Pflege	114
Personalwesen	107
Adresshandel, Werbung	94
Polizei, Strafverfahren, Justiz, Verfassungsschutz	87
Kreditwirtschaft	86
Soziales	74
Verkehr	65
Handel, Handwerk, Gewerbe	57
Versicherungen	42
Versorgungsunternehmen	34
Vereine und Verbände	23
Forschung, Statistik	17
IT-Sicherheit + DV-Technik + Herstelleranfragen	15
Rundfunk, Fernsehen, Presse	11
Sonstiges	43
Summe der dokumentierten Eingaben	**1.860**
Summe der dokumentierten Beratungen	**231**
davon Eingaben und Beratungen Videobeobachtung betreffend	394
Summe telefonischer Eingaben und Beratungen	**3.708**
Gesamtsumme	**5.799**

1.5

Bußgelder und Informationspflicht nach § 42a BDSG 2016

1.5.1

Bußgelder

Bedingt durch die Belastungen im Rahmen der Umsetzungsarbeiten der neuen EU-Datenschutzvorgaben konnten im Berichtsjahr nur 15 Bußgeldverfahren abgeschlossen werden. Es waren keine spektakulären Fälle darunter. Den Verfahren lagen sechs Verstöße gegen Pflichten der verantwortlichen Stellen gegenüber Betroffenen bzw. der Aufsichtsbehörde oder Verstöße gegen Meldeverpflichtungen zugrunde (Tatbestände des § 43 Abs. 1 BDSG). Die übrigen neun Verfahren bezogen sich auf Vorfälle wegen unzulässiger Datenerhebung (Tatbestände des § 43 Abs. 2 BDSG). Zwei Verfahren wurden mit einem rechtskräftigen Bußgeldbescheid beendet. Dabei wurden Bußgelder in Höhe von 2.500 EUR verhängt.

1.5.2

Informationspflicht nach § 42a BDSG

Im Berichtsjahr gingen insgesamt 65 Meldungen nach § 42a BDSG wegen unrechtmäßiger Kenntniserlangung von Daten bei mir ein. Davon erfolgten 24 Meldungen vorsorglich. In diesen Fällen bestand keine Informationspflicht. In 41 Fällen war der Tatbestand einer Datenschutzrechtsverletzung allerdings erfüllt. Die meisten Fälle betrafen den Fehlversand von Schreiben/E-Mails mit personenbezogenen Daten oder eine sonstige Übermittlung von personenbezogenen Daten an unberechtigte Dritte.

Von der in Hessen ansässigen Betreiberfirma für EC-Karten-Terminals erhielt ich 23 Meldungen über (bundesweite) Vorfälle, in denen es zu Diebstählen oder Manipulationen von bzw. an Electronic-Cash-Terminals gekommen ist. Die restlichen Meldungen bezogen sich auf Vorfälle wie: versuchte Hackerangriffe, Diebstähle z. B. von Konto- und Kundenunterlagen oder Firmenhandys, Einsichtnahme auf Kontodaten eines Dritten beim Online-Banking u. Ä.

2. Europa und Internationales

2.1

Koordinierte Kontrollgruppe für das SIS II

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrung der Interessen der Landesdatenschutzbeauftragten in der Koordinierten Kontrollgruppe für das SIS II übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an zwei Sitzungen in Brüssel teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2016 dar.

Zur Sicherstellung der Koordination der Aufsicht für das Schengener Informationssystem der zweiten Generation (SIS II) treffen sich die Vertreter der nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte (EDSB) zweimal jährlich. Darüber hinaus gehören die nationalen Datenschutzbehörden Islands, Liechtensteins, Norwegens und der Schweiz zu dieser Gruppe, da diese Länder aufgrund von Assoziierungsabkommen gleichfalls an dem Informationssystem teilnehmen. Den Vorsitz der Gruppe hat derzeit die portugiesische Datenschutzbehörde, den stellvertretenden Vorsitz die maltesische Datenschutzbehörde inne.

2.1.1

Ausschreibungen von gestohlenen Kraftfahrzeugen im SIS II

Wichtig aus deutscher Sicht war weiterhin die Behandlung des Problems der Ausschreibungen von gestohlenen oder sonst abhandengekommenen Kraftfahrzeugen (s. 44. Tätigkeitsbericht, Ziff. 2.1.1). Der Erwerb eines Kraftfahrzeugs, das im SIS II als gestohlen oder abhandengekommen ausgeschrieben ist, bringt zahlreiche Probleme mit sich. Der Erwerber, der von der Ausschreibung im Zeitpunkt des Kaufs in der Regel keine Kenntnis hat, hat beispielsweise Schwierigkeiten beim Weiterverkauf des Fahrzeugs oder bei Reisen im Schengen-Raum. Die umstrittene Frage ist, ob die Ausschreibung gelöscht werden kann, wenn das Fahrzeug gefunden wurde, oder ob es neben dem Auffinden weiterer Voraussetzungen für die Löschung bedarf. Die Auslegung des Art. 38 des Beschlusses 2007/533/JI ist für diese Frage entscheidend.

> Art. 38 SIS II Beschluss 2007/533/JI
>
> (1) Daten in Bezug auf Sachen, die zur Sicherstellung oder Beweissicherung in Strafverfahren gesucht werden, werden in das SIS II eingegeben.
>
> (2) Es werden folgende Kategorien von leicht identifizierbaren Sachen einbezogen:
>
> a) Kraftfahrzeuge mit einem Hubraum von mehr als 50 ccm, Wasserfahrzeuge und Luftfahrzeuge;
>
> …

Nachdem die Delegationen bereits in mehreren Sitzungen der Kontrollgruppe über die Auslegung der Norm diskutiert hatten, verständigten sie sich bei der Frühjahrssitzung auf die Annahme einer gemeinsamen Stellungnahme zu der Thematik (https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Large_IT_systems/SIS/16-05-24 SIS II_SCG_Common_Position_on_Deletion_of_Alerts_on_Stolen_Vehicles_EN.pdf). Die Kontrollgruppe vertritt die Auffassung, dass das bloße Auffinden des Fahrzeugs nicht Grundlage für eine Löschung einer Ausschreibung sein kann. Vielmehr führt das Auffinden des Fahrzeugs zur Notwendigkeit des Austauschs weiterer Informationen zwischen den betreffenden Mitgliedstaaten, bevor es zu einer Löschung kommen kann. Die Zusammenarbeit zwischen den Mitgliedstaaten ist daher von entscheidender Bedeutung, um die Rechte der betroffenen Personen zu wahren. Nicht nur der Erwerber des Fahrzeugs ist in diesen Fallkonstellationen in seinen Rechten beeinträchtigt, sondern in der Regel auch diejenige Person, bei der das Fahrzeug abhandengekommen ist. Vor diesem Hintergrund ist es nach Auffassung der Kontrollgruppe unabdingbar, dass ein verbindlicher Maßnahmenkatalog erstellt wird, der den betreffenden Mitgliedstaaten als Grundlage einer effizienten Zusammenarbeit dient. Ferner sollten alle Mitgliedstaaten auf nationaler Ebene die Verantwortlichkeiten für den Umgang mit Ausschreibungen im SIS klar zuordnen und die entsprechenden Personen durch geeignete Trainings schulen. Nur so könne eine reibungslose Zusammenarbeit gewährleistet werden.

2.1.2

Nutzung von Daten des SIS II für Verwaltungszwecke

Eine wichtige Frage aus deutscher Sicht war außerdem die potenzielle Nutzung von SIS II-Daten für Verwaltungszwecke. Mehrere Mitgliedstaaten warfen die Frage auf, zu welchem Zweck die in die SIS II-Datenbank eingegebenen Daten durch die nationalen Behörden verwendet werden dürfen. Diskutiert wurde unter anderem die Nutzung von SIS II-Daten durch die zuständigen Behörden eines Mitgliedstaats im Zusammenhang mit der Erteilung eines Waffenscheins. Die hierzu einschlägige Vorschrift findet sich in Art. 46 des Beschlusses 2007/533/JI über die Errichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation.

> Art. 46 SIS II Beschluss 2007/533/JI
>
> (1) Die Mitgliedstaaten dürfen die in den Artikeln 20, 26, 32, 34, 36 und 38 genannten Daten nur für die der jeweiligen Ausschreibung entsprechenden Zwecke verarbeiten.
> ...
> (5) Hinsichtlich der Ausschreibungen nach den Artikeln 26, 32, 34, 36 und 38 dieses Beschlusses muss jede Verarbeitung der (…) Informationen zu anderen Zwecken als jenen, zu denen die Ausschreibung in das SIS eingegeben wurde, in Verbindung mit einem spezifischen Fall stehen und ist nur zulässig, soweit dies zur Abwehr einer schwerwiegenden und unmittelbar bevorstehenden Gefahr für die öffentliche Sicherheit und Ordnung oder aus schwerwiegenden Gründen der Sicherheit des Staates oder zur Verhütung einer Straftat mit erheblicher Bedeutung erforderlich ist. …
>
> (6) Die Daten dürfen nicht zu Verwaltungszwecken genutzt werden.

Grundsätzlich dürfen demnach die Daten nur für die der Ausschreibung entsprechenden Zwecke verarbeitet werden, es sei denn, es liegt ein Ausnahmefall gemäß Art. 46 Abs. 5 vor. Wie bereits dem Wortlaut der Regelung des Absatzes 5 zu entnehmen ist, ist dies eine eng auszulegende und auf besondere Einzelfälle begrenzte Ausnahmevorschrift. Absatz 6 statuiert daneben ein generelles, das heißt ausnahmsloses Verbot der Datenverwendung zu Verwaltungszwecken.

Die Koordinierte Kontrollgruppe für das SIS II wird sich in den kommenden Monaten mit der Frage der Definition der „Verwaltungszwecke“ auseinandersetzen. Dabei wird auch zu hinterfragen sein, ob ein bestimmtes behördliches Handeln von allen Mitgliedstaaten als Verwaltungshandeln im Sinne des Absatzes 5 zu verstehen ist. Hierzu werde ich im kommenden Tätigkeitsbericht ausführlich berichten.

2.2
Gemeinsame Kontrollinstanz Europol

Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat dem Hessischen Datenschutzbeauftragten die Wahrung der Interessen der Landesdatenschutzbeauftragten in der Gemeinsamen Kontrollinstanz für Europol übertragen. Meine Mitarbeiterin hat im Berichtszeitraum an drei Sitzungen in Brüssel sowie an verschiedenen Treffen der Arbeitsgruppe „Neue Projekte“ in Den Haag teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2016 dar.

2.2.1
Neue Rechtsgrundlage für Europol

Über den Entwurf für eine neue Rechtsgrundlage für Europol und die hierzu erfolgten Stellungnahmen der Gemeinsamen Kontrollinstanz (GKI) habe ich in verschiedenen Tätigkeitsberichten, zuletzt im 44. Tätigkeitsbericht (Ziff. 2.2), berichtet.

Die neue Europol-Verordnung [VO (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung vom 11.05.2016, ABl. EU vom 24.05.2016, S. 53 ff.] ist nunmehr in Kraft getreten und gilt ab dem 01.05.2017, d. h., sie ist ab diesem Zeitpunkt anzuwenden.

Eines der aus datenschutzrechtlicher Sicht wichtigsten und bis zuletzt umstrittenen Themen war dabei die künftige datenschutzrechtliche Kontrolle von Europol. Diese wurde folgendermaßen geregelt:
Primär zuständig für die Kontrolle von Europol ist nicht mehr die Gemeinsame Kontrollinstanz (GKI), sondern der Europäische Datenschutzbeauftragte (EDSB).

> Art. 43 Abs. 1 Europol-Verordnung
>
> Der EDSB ist zuständig für die Kontrolle und Sicherstellung der Anwendung dieser Verordnung zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Europol sowie für die Beratung von Europol und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten. Zu diesem Zweck erfüllt er die in Absatz 2 genannten Aufgaben und übt die in Absatz 3 festgelegten Befugnisse in enger Zusammenarbeit mit den nationalen Kontrollbehörden gemäß Artikel 44 aus.

Der EDSB ist aber bei vielen Aktivitäten verpflichtet, mit den nationalen Kontrollbehörden zusammenzuarbeiten. Diese Einbeziehung ist deshalb wichtig, weil der größte Teil der bei Europol gesammelten und verarbeiteten Daten aus den Mitgliedstaaten stammt.

> Art. 44 Abs. 1 bis 3 Europol-Verordnung
>
> (1) Bei Fragen, die eine Einbeziehung der Mitgliedstaaten erfordern, arbeitet der EDSB eng mit den nationalen Kontrollbehörden zusammen, vor allem, wenn der EDSB oder eine nationale Kontrollbehörde größere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten oder möglicherweise unrechtmäßige Übermittlungen über die Informationskanäle von Europol feststellt, oder bei Fragen einer oder mehrerer nationaler Kontrollbehörden zur Umsetzung und Auslegung dieser Verordnung.
>
> (2) Der EDSB nutzt bei der Wahrnehmung seiner Pflichten gemäß Artikel 43 Absatz 2 die Fachkenntnisse und Erfahrungen nationaler Kontrollbehörden. Bei der Wahrnehmung gemeinsamer Inspektionen mit dem EDSB haben die Mitglieder und Bediensteten der nationalen Kontrollbehörden unter gebührender Berücksichtigung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit die Befugnisse, die den Befugnissen nach Artikel 43 Absatz 4 entsprechen, und sind entsprechend der Verpflichtung nach Artikel 43 Absatz 6 verpflichtet. Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen der EDSB und die nationalen Kontrollbehörden einschlägige Informationen aus und unterstützen sich gegenseitig bei Überprüfungen und Inspektionen.
>
> (3) Der EDSB unterrichtet die nationalen Kontrollbehörden regelmäßig über alle Fragen, die sie unmittelbar betreffen oder in sonstiger Hinsicht für sie relevant sind. Auf Antrag einer oder mehrerer nationaler Kontrollbehörden unterrichtet der EDSB sie über spezielle Fragen.

Neben dieser punktuellen Zusammenarbeit mit verschiedenen nationalen Aufsichtsbehörden, zu der auch die Durchführung gemeinsamer Inspektionen gehören kann, ist eine formalisierte Zusammenarbeit in einem sog. Beirat für die Zusammenarbeit (Cooperation Board) vorgesehen. In diesem Beirat sind Delegierte der nationalen Aufsichtsbehörden und der EDSB vertreten.

> Art. 45 Europol-Verordnung
>
> (1) Es wird ein Beirat für die Zusammenarbeit eingesetzt, dem eine Beratungsfunktion zukommt. Er besteht aus je einem Vertreter einer nationalen Kontrollbehörde jedes Mitgliedstaats und dem EDSB.
>
> (2) Der Beirat für die Zusammenarbeit handelt bei der Ausführung seiner Aufgaben gemäß Absatz 3 unabhängig, fordert von niemandem Weisungen an und nimmt auch keine Weisungen entgegen.
>
> (3) Der Beirat für die Zusammenarbeit hat folgende Aufgaben:
>
> a) Erörterung der allgemeinen Politik und Strategie Europols im Bereich der Überwachung des Datenschutzes und der Zulässigkeit der Übermittlung und des Abrufs personenbezogener Daten sowie der Mitteilung von personenbezogenen Daten an Europol durch die Mitgliedstaaten;
> b) Prüfung von Schwierigkeiten bei der Auslegung oder Anwendung dieser Verordnung;
> c) Untersuchung allgemeiner Probleme im Zusammenhang mit der Ausübung der unabhängigen Überwachung oder der Ausübung der Rechte der betroffenen Personen;
> d) Erörterung und Ausarbeitung harmonisierter Vorschläge für gemeinsame Lösungen in den in Artikel 44 Absatz 1 genannten Fragen;
> e) Erörterung der vom EDSB gemäß Artikel 44 Absatz 4 vorgelegten Fälle;
> f) Erörterung der von den nationalen Kontrollbehörden vorgelegten Fälle und
> g) Förderung der Sensibilisierung für Datenschutzrechte.
>
> (4) Der Beirat für die Zusammenarbeit kann Stellungnahmen, Leitlinien und Empfehlungen formulieren und bewährte Verfahren festlegen. Der EDSB und die nationalen Kontrollbehörden tragen ihnen im Rahmen ihrer jeweiligen Zuständigkeiten und unter Wahrung ihrer Unabhängigkeit umfassend Rechnung.
>
> (5) Der Beirat für die Zusammenarbeit tritt nach Bedarf, mindestens jedoch zweimal jährlich zusammen. Die Kosten und die Ausrichtung seiner Sitzungen übernimmt der EDSB.
>
> (6) Der Beirat für die Zusammenarbeit nimmt in seiner ersten Sitzung mit einfacher Mehrheit seiner Mitglieder seine Geschäftsordnung an. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt.

Die GKI hat einen Entwurf für eine Geschäftsordnung des noch zu errichtenden Gremiums erarbeitet. Dieser Entwurf wurde dem EDSB übersandt und wird demnächst mit ihm und seinen Mitarbeitern diskutiert. Darin ist u. a. vorgesehen, dass in jenen Ländern, in denen mehrere Aufsichtsbehörden existieren – wie in Deutschland –, ein gemeinsamer Vertreter bestimmt werden soll, der wiederum einen Vertreter hat, der in den Sitzungen anwesend sein kann. Damit soll weiterhin sichergestellt werden, dass neben der Vertretung durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz auch eine Vertretung der Bundesländer durch eine oder einen der Landesbeauftragten erfolgen kann.

2.2.2
Liste der am meisten gesuchten Personen

Im 44. Tätigkeitsbericht (Ziff. 2.2.3) hatte ich von dem Vorhaben von Europol berichtet, eine Liste mit den am meisten gesuchten Personen (Most Wanted-List) auf der Internetseite von Europol zu veröffentlichen. Die Daten sollen von jenen Mitgliedstaaten geliefert werden, die auf nationaler Ebene über eine derartige Liste verfügen. Die Arbeitsgruppe „Neue Projekte“ der GKI, in der meine Mitarbeiterin vertreten ist, hat sich mit dem Vorhaben von Europol befasst und über Einzelheiten mit den zuständigen Mitarbeitern von Europol in Den Haag mehrmals gesprochen. Die Mitglieder der Arbeitsgruppe sind der Auffassung, dass eine derartige Liste nicht bei Europol betrieben werden kann, wenn davon auszugehen ist, dass Europol selbst diese Daten verarbeitet. Für eine derartige Verarbeitung bestehe keine Rechtsgrundlage im Europol-Beschluss (Beschluss des Rates zur Errichtung des Europäischen Polizeiamts vom 06.04.2009, 2009/371/JI). Ein derartiges Vorhaben sei aber realisierbar, wenn die Datenverarbeitung beispielsweise bei den Mitgliedstaaten oder anderen Stellen läge.

Ungeachtet dieser Rechtsauffassung wurde die Most Wanted-List bereits Ende Januar d. J. von Europol auf seiner Internetseite veröffentlicht. Derzeit wird an einer Lösung gearbeitet, bei der die Liste bei ENFAST (European Network of Fugitive Active Search Teams) geführt wird. Bei ENFAST handelt es sich um das Netzwerk europäischer Zielfahndungsdienststellen, zu deren Aufgaben die Lokalisierung und Festnahme international gesuchter, schwerstkrimineller Straftäter gehören.

2.2.3
Aktivitäten von Europol im Internet

Ein weiteres Thema betrifft die Recherche von Europol im Internet. Bei den Kontrollen fand die GKI immer wieder Hinweise darauf, dass Mitarbeiter von Europol nicht nur in öffentlich zugänglichen Bereichen des Internets recherchieren, sondern auch in solchen, die nur durch besondere Maßnahmen erschlossen werden können. Welche Methoden Europol im Einzelnen anwendet, um Zugang zu für den normalen Nutzer versteckten Inhalten und bestimmten Plattformen im sog. Darknet zu erhalten, muss noch aufgeklärt werden. Aus rechtlicher Sicht ist jedoch die Grenze für derartige Aktivitäten dann erreicht, wenn die Art und Weise, wie die Recherchen erfolgen, als Zwangsmaßnahmen einzuordnen sind. Europol ist es verwehrt, Zwangsmaßnahmen anzuwenden, was ausschließlich die zuständigen Behörden der Mitgliedstaaten dürfen. Dies ergibt sich aus der Europol betreffenden Bestimmung des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

> Art. 88 Abs. 3 AEUV
>
> Europol darf operative Maßnahmen nur in Verbindung und in Absprache mit den Behörden des Mitgliedstaats oder der Mitgliedstaaten ergreifen, deren Hoheitsgebiet betroffen ist. Die Anwendung von Zwangsmaßnahmen bleibt ausschließlich den zuständigen einzelstaatlichen Behörden vorbehalten.

Auch aus Erwägungsgrund 7 des Europol-Beschlusses folgt, dass dem Europol-Personal von Europol keine Vollzugsgewalt übertragen werden darf. In der neuen Europol-Verordnung wird dies ebenfalls klargestellt:

> Art. 4 Abs. 5 Europol-Verordnung
>
> Bei der Durchführung ihrer Aufgaben wendet Europol keine Zwangsmaßnahmen an.

2.2.4
Kontrolle von Europol

Die GKI hat im Berichtszeitraum wieder die regelmäßige jährliche Kontrolle durchgeführt. Der Bericht über diese Kontrolle ist vertraulich. Da im nächsten Jahr der Wechsel von der GKI zum EDSB erfolgen wird, soll eine weitere Kontrolle erfolgen, in der es um die Frage geht, inwieweit Europol die von der GKI ausgesprochenen Empfehlungen umgesetzt hat.

2.3

Privacy Shield

Auch in diesem Jahr waren die Folgen des Urteils des EuGH vom 06.10.2015, mit dem dieser die Safe-Harbor-Entscheidung der Europäischen Kommission für nichtig erklärt hat, ein großes Thema auf der Agenda nicht nur des Hessischen Datenschutzbeauftragten, sondern auch der DSK sowie der Artikel 29-Gruppe auf europäischer Ebene.*

Wie in meinem letzten Tätigkeitsbericht (Ziff. 1.3) dargestellt, handelte es sich bei Safe Harbor um ein Instrument, mit dem es vor allem Unternehmen ermöglicht werden sollte, auf einfachem Wege Daten in die USA zu transferieren. Durch eine Selbstzertifizierung sollten US-Unternehmen sicherstellen, dass die Daten bei ihnen angemessen geschützt sind und die Betroffenen auch gegenüber den zertifizierten US-Unternehmen ihre Rechte auf Information über den Umgang mit ihren Daten, Auskunft und gegebenenfalls Löschung ausüben können.

Am 29.02.2016 hat die Europäische Kommission das Ergebnis ihrer Verhandlungen mit den USA in Form eines Entwurfs einer Entscheidung der Europäischen Kommission zum sogenannten EU-US-Privacy Shield veröffentlicht. Der EU-US-Privacy Shield sollte an die Stelle der aufgehobenen Safe-Harbor-Entscheidung treten. Bevor die Europäische Kommission in dieser Sache eine endgültige Entscheidung getroffen hat, konsultierte sie die EU-Mitgliedstaaten sowie die in der sogenannten Artikel 29-Datenschutzgruppe vereinten Datenschutzbehörden Europas. Der Hessische Datenschutzbeauftragte hat sich an der Bewertung der vorgelegten Texte intensiv beteiligt.

Die Artikel 29-Datenschutzgruppe hat den Entscheidungsentwurf der Europäischen Kommission zum EU-US-Privacy Shield einer Bewertung unterzogen und am 13.04.2016 ihre Stellungnahme (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf) sowie eine begleitende Pressemitteilung veröffentlicht. Sie stellte fest, dass der erste Entwurf des Privacy Shield im Vergleich zu der vom Europäischen Gerichtshof aufgehobenen Vorgängerregelung "Safe Harbor" eine Reihe von Verbesserungen im Hinblick auf den Schutz personenbezogener Daten enthielt. Gleichzeitig begegneten einige Punkte jedoch noch erheblichen Bedenken. Die Artikel 29-Gruppe hat die Europäische Kommission daher aufgefordert, auf diese Bedenken zu reagieren und durch entsprechende Änderungen sicherzustellen, dass der Privacy Shield ein angemessenes Datenschutzniveau gewährleistet.

Nachdem der erste Entwurf des Privacy Shield noch einmal überarbeitet worden war, hat die Europäische Kommission am 13.07.2016 den EU-US-Privacy Shield verabschiedet. Zu der Entscheidung der Europäischen Kommission hat sich die Artikel 29-Datenschutzgruppe noch einmal kritisch geäußert. Da der Beschluss der Europäischen Kommission zum EU-US-Privacy Shield jedoch bindend ist, kann der Privacy Shield nun trotz der von den Datenschutzbehörden geäußerten Kritik an den Regelungen genutzt werden, um Daten aus Europa an die bereits zertifizierten Unternehmen zu transferieren, sofern auch die weiteren Anforderungen an den Datentransfer erfüllt werden. Die für den Datenexport verantwortlichen europäischen Stellen haben dabei stets darauf zu achten, dass das Unternehmen, das die Daten empfängt, auch tatsächlich auf der Liste des US-Handelsministeriums erscheint. Darüber hinaus ist sicherzustellen, dass sich die Zertifizierung auch auf die Kategorie von Daten (Beschäftigtendaten = "HR" oder sonstige Daten "non HR") bezieht, die übermittelt werden soll.

Ein Leitfaden für Bürgerinnen und Bürger, herausgegeben von der Europäischen Kommission, in dem vor allem die Rechte Betroffener unter dem EU-US-Privacy Shield dargestellt werden, ist unter http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf auch in deutscher Sprache verfügbar.

Weitere Informationen zum Privacy Shield für Unternehmen und betroffene Bürgerinnen und Bürger sowie Beschwerdeformulare werden zurzeit von der Artikel 29-Gruppe erarbeitet. Sobald diese zur Verfügung stehen, werden diese auf der Webseite des Hessischen Datenschutzbeauftragten bereitgestellt werden.

---

* Die Artikel 29-Datenschutzgruppe besteht aus Vertretern der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten, dem Europäischen Datenschutzbeauftragten und einem nicht stimmberechtigten Vertreter der Europäischen Kommission. Sie berät die Europäische Kommission und hat zur einheitlichen Anwendung der Vorschriften der Datenschutzrichtlinie beizutragen. Sie ist unabhängig und trifft ihre Entscheidungen nach dem Mehrheitsprinzip.

2.4

DS-GVO:
Ziele und Aufgaben der IT Task Force im Jahr 2016

Auf der Grundlage des Arbeitsplans für 2016[1] *der Art. 29-Gruppe (WP29, entsprechend der bisherigen Europäischen Datenschutz-Richtlinie) ist für 18 Monate eine sogenannte IT Task Force eingerichtet worden, in der meine Mitarbeiterin Deutschland repräsentiert. Der*

IT Task Force ist das Mandat erteilt, eine geeignete IT-Infrastruktur zu finden und bis Mai 2018 bereitzustellen, um die durch Art. 60 bis Art. 66 DS-GVO vorgegebenen Aufgaben der Aufsichtsbehörden und des Sekretariats des Europäischen Datenschutzbeauftragten mit IT zu unterstützen.

Die IT-Infrastruktur muss auf einem Baukastenprinzip beruhen. Jeder Baustein kann aus einem oder mehreren IT-Systemen bestehen. Zu bestimmende Bausteine müssen jeweils einer Basisfunktion dienen, um die Zusammenarbeit, insbesondere den Austausch von Dokumenten, bis zur Abstimmung und einer entsprechenden Entscheidung zwischen den Europäischen Datenschutz-Aufsichtsbehörden zu unterstützen. Denn es sind z. B. länderübergreifend Datenschutzfragen und -eingaben zu bearbeiten. Gegenseitige Amtshilfe („mutual assistance“) und ein gemeinsames Einschreiten bei Datenschutzverstößen („joint investigations“) sind Formen der Zusammenarbeit. Sicherlich gehört dazu auch vorrangig die Unterstützung des Kohärenzverfahrens („consistency mechanism“).

Ein weiterer wesentlicher Teil des Mandats ist die Bereitstellung eines „One-Stop-Shops“ (OSS), über den Bürgerinnen und Bürger ihre Anfragen und Eingaben an die Datenschutz-Aufsichtsbehörden in jedem europäischen Land richten können – unabhängig davon, gegen wen sich die Eingabe richtet und an welchem Ort sich die datenverarbeitende Stelle befindet. Aus Sicht der Bürgerinnen und der Bürger muss der OSS einen von überall in der EU erreichbaren Web-basierten Zugriff realisieren.

Die Verfahren, die in der DS-GVO beschrieben sind, sind durch Basisfunktionen (engl. building blocks) in technischen Prozessen abzubilden. Die IT-Infrastruktur muss so gestaltet sein, dass sowohl die Verfahren als auch die technischen Prozesse für alle Beteiligten nachvollziehbar sind.

Mittels eines Fragebogens sind die ersten Vorstellungen evaluiert worden, welche technischen Bedingungen zu berücksichtigen sind. Im Fragebogen wurde nach speziellen Anforderungen gefragt, die die Systemarchitektur beeinflussen. Dazu gehörten:

- Fragen zur IT-Sicherheit,
- nach der Möglichkeit, eine Cloud-Lösung bei ggf. auch externen Anbietern einzusetzen, und
- zu Formen und zu Zeitpunkten der Veröffentlichung offizieller Dokumente, die aus einer der Arten der Zusammenarbeit hervorgehen.

Ein entsprechender Fragebogen ist an alle Datenschutz-Aufsichtsbehörden der zu diesem Zeitpunkt 28 EU-Mitgliedstaaten, an Norwegen und an den Europäischen Datenschutzbeauftragten verschickt worden. Die IT Task Force erhielt 23 Rücksendungen. Die Auswertung der Antworten ergab die folgende Priorisierung, welche Basisfunktionen zu implementieren sind (Tabelle: Zur Notwendigkeit von Basisfunktionen).

Basisfunktionen	Erforderlich („Must“)
Austausch von Dokumenten	87%
Nachvollziehbare Kommunikation zwischen den Aufsichtsbehörden	78 %
Verwaltung von übergreifenden Fällen („case management“)	78 %
Unterstützung der Abstimmungsprozesse	48 %
Veröffentlichung von offiziellen Dokumenten auf einer entsprechenden Web-Site	35 %

Tabelle: Zur Notwendigkeit von Basisfunktionen

Auf Betreiben der EU-Kommission sind parallel zur Evaluation der zurückgesendeten Fragebogen sechs bestehende IT-Systeme der IT Task Force vorgestellt worden, die in unterschiedlichen Bereichen der EU-Verwaltung bereits eingesetzt werden und die ggf. in Betrachtungen einzubeziehen sind. Das Ziel der Untersuchung sollte sein, eine Einschätzung zu treffen, ob es bereits ein solches IT-System in der EU-Verwaltung gibt, das sich mit einer geringeren Anzahl von Änderungen nutzen lässt.

Die IT Task Force hatte zu keinem Zeitpunkt die Absicht, eine vollständige oder gar eigene IT-Infrastruktur zu entwickeln, obwohl die Unabhängigkeit des EDPS gewahrt sein muss. Aus dieser Situation heraus wird eine weitere Analyse notwendig, mit welchem Aufwand es möglich ist, die genannten, priorisierten Anforderungen zu erhalten („gap analysis“). Trotz der Einflussnahme der unterschiedlichen Interessengruppen ist zu erwarten, dass – entsprechend des Plans – eine technische Analyse für eine geeignete IT-Infrastruktur bestehend aus mehreren identifizierten Basisfunktionen (building blocks) durch die IT Task Force im Dezember 2016 geliefert wird. Die Arbeit der IT Task Force wird im Jahr 2017 fortgesetzt.

---

[1] WP29 action plan 2016 for the implementation of the GDPR

3. Datenschutz im öffentlichen Bereich

3.1

Landesverwaltung

3.1.1

Datenschutzrechtliche Überprüfung der polizeilichen Falldatei „Rauschgift“ – auch Bagatellfälle werden erfasst

Bei Überprüfung der sog. Falldatei „Rauschgift“, in welcher bundesweit bedeutsame Rauschgiftdelikte gespeichert werden, ist aufgefallen, dass entgegen den gesetzlichen Vorgaben auch Bagatelldelikte erfasst wurden und oftmals die Entscheidung über die Speicherung in dieser Datei nicht gründlich genug dokumentiert wurde.

Die Falldatei „Rauschgift“ ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt BKA) geführt. Alle Landespolizeien und auch die Zollfahndung haben Zugriff auf die Datei und können Daten direkt einspeichern und abrufen. Zusammen mit der Bundesdatenschutzbeauftragten und einigen anderen Landesdatenschutzbehörden habe ich im Jahr 2015 und 2016 die Datei stichprobenartig überprüft. Im Rahmen der Kontrollen wurden sowohl die Gesamtstruktur der Datei als auch Einzelspeicherungen überprüft.

Rechtliche Voraussetzungen

Die Rechtsgrundlagen für diese Datei finden sich im BKAG. So erlaubt § 8 Abs. 1 BKAG, dass das BKA zur Erfüllung seiner Aufgaben aus § 2 Abs. 1 BKAG personenbezogene Daten in Dateien speichern, verändern und nutzen kann. Dies umfasst u. a. die Personaldaten, Daten über den Tatort, die Tatzeit und den Tatvorwurf. Weitere personenbezogene Daten können gemäß § 8 Abs. 2 BKAG gespeichert werden, wenn Grund zur Annahme besteht, dass der Betroffene weitere Straftaten begeht. Es muss also eine sog. Negativprognose vorliegen. Diese Prognose muss in jedem Einzelfall von der Polizei erstellt werden. Die einzelnen Gründe und das Ergebnis müssen nachvollziehbar dokumentiert sein. Nach § 2 Abs. 1 BKAG muss es sich bei den Straftaten, bei denen das BKA die Polizei des Bundes und der Länder unterstützt und folglich auch personenbezogene Daten in Dateien speichern darf, um Fälle mit länderübergreifender, internationaler oder erheblicher Bedeutung handeln. Ob jeweils die Voraussetzungen dieser Vorschriften bei den Speicherungen für die Falldatei „Rauschgift“ vorlagen, war Gegenstand meiner Prüfung.

> § 2 Abs. 1 BKAG
>
> Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung.
>
> § 8 Abs. 1 und 2 BKAG
>
> (1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 bis 3
> 1. die Personendaten von Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale,
> 2. die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,
> 3. die Tatzeiten und Tatorte und
> 4. die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten in Dateien speichern, verändern und nutzen.
>
> (2) Weitere personenbezogene Daten von Beschuldigten und personenbezogene Daten von Personen, die einer Straftat verdächtig sind, kann das Bundeskriminalamt nur speichern, verändern und nutzen, soweit dies erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind.

In der Datei speichern die Polizeibehörden in Bund und Ländern in der Regel alle Fälle im Kontext von Rauschgiftdelikten. Gespeichert werden Angaben zu Tatverdächtigen, zu deren Tatbeteiligung, zum Tatort, Tatmittel, erstrebtem bzw. erlangtem Gut, eine Fallbeschreibung und eventuell weitere Informationen.

Ergebnis der Prüfung

Bei meinen Kontrollen in drei verschiedenen Polizeipräsidien wurden stichprobenartig insgesamt ca. 45 Akten überprüft, welche für die Aufnahme in diese Datei von dem jeweiligen Präsidium gemeldet wurden. Die endgültige Entscheidung über eine Speicherung erfolgt durch das Landeskriminalamt.

Aufgrund der Art der Aktenauswahl und der eher geringen Anzahl war die Stichprobe nicht unbedingt repräsentativ. Allerdings entsprechen meine Feststellungen in weiten Teilen denen der Prüfung anderer Landesdatenschutzbeauftragter.

Ich habe festgestellt, dass die Polizei einheitlich nach einem Kriterienkatalog vorgeht. Danach werden alle Vorgänge in der Falldatei „Rauschgift“ erfasst, in denen der Betroffene mit Rauschgift handelt oder es zu einem Rauschgifttodesfall gekommen ist. Ebenso erfasst werden Konsumenten harter Drogen mit Sicherstellung von über einem Gramm (Heroin, Kokain, Crack, Amphetamin, Ecstasy und LSD), Diebstähle von Betäubungsmitteln aus Apotheken sowie Rezeptfälschungen. Bei Cannabis muss die Mindestmenge für die Erfassung zehn Gramm betragen. Für die Meldung an das Landeskriminalamt (LKA) genügt als Voraussetzung ein sog. begründeter Tatverdacht.

Auffallend bei der Prüfung war eine nicht unerhebliche Anzahl von Einzelfällen, bei denen eine Rauschgiftmeldung gemacht wurde, das Vorliegen der Voraussetzungen des § 8 Abs. 2 BKAG jedoch zweifelhaft erschien. So gab es z. B. sieben Fälle, bei denen Rauschgift nur für den Eigengebrauch (geringe Mengen, überwiegend Marihuana) im Besitz war, einige Personen hiervon waren auch noch minderjährig, so dass die Voraussetzungen des § 8 Abs. 2 BKAG als nicht gegeben angesehen werden können und auch im Rahmen der Verhältnismäßigkeit die Notwendigkeit der Speicherung zumindest offen bleibt. So wurden etwa zwei Personen von Familienangehörigen angezeigt, eine Person hat sich selbst angezeigt. Diese Anzeigen waren eher als „Erziehungsmaßnahmen“ der Eltern zu werten und waren nicht dem Bereich der schweren Drogenkriminalität zuzuordnen.

Ebenso gab es eine Handvoll Fälle, bei denen ein begründeter Tatverdacht nicht festgestellt werden konnte. Oftmals handelte es sich um (anonyme) Anzeigen, bei denen nach Hausdurchsuchungen jedoch keine Drogen aufgefunden werden konnten und die Verfahren eingestellt wurden. Die Voraussetzungen für eine Speicherung in der Falldatei „Rauschgift“ waren auch hier offensichtlich nicht gegeben.

Weiterhin war aufgefallen, dass die Entscheidung für eine Rauschgiftmeldung in vielen Fällen nicht ausreichend dokumentiert wurde. In den Akten befand sich oftmals nur ein ausgefülltes Formblatt für die Meldung. Aus den Unterlagen ging jedoch nicht hervor, ob den zuständigen Beamten die Rechtsgrundlage der Speicherung mit den einzelnen Voraussetzungen bewusst war und angewendet wurde und weshalb tatsächlich von einer Negativprognose auszugehen war.

Konsequenzen für den künftigen Umgang mit Verbunddateien

Nach Abschluss der Prüfungen habe ich mit dem LKA und dem Hessischen Ministerium des Innern und für Sport ein Gespräch über die Ergebnisse geführt. Es wurde vereinbart, dass künftig Eingaben in die Verbunddatei genauer dokumentiert werden (insbesondere hinsichtlich der Prognoseentscheidung), um den Anforderungen an die Vollständigkeit und Nachvollziehbarkeit der Aktenführung gerecht zu werden. Weiterhin wurde zugesagt, die Vorgehensweise zur Umsetzung der Verfahrensausgangsmitteilung der Staatsanwaltschaft zu überarbeiten, damit auch regelmäßig durch das LKA die Löschung von Datensätzen bei Wegfall der Speichervoraussetzungen veranlasst werden kann.

Die Feststellungen der an der gemeinsamen Prüfung beteiligten Datenschutzbeauftragten wurden in einem gemeinsamen Prüfbericht zusammengefasst. Dieser wurde u. a. der Innenministerkonferenz, der Justizministerkonferenz sowie den entsprechenden Fachausschüssen des Bundestages zur Verfügung gestellt.

Gleichzeitig hat die Datenschutzkonferenz dies zum Anlass genommen, auf die festgestellten Probleme bei der Praxis der polizeilichen Speicherungen im Rahmen einer Entschließung aufmerksam zu machen (vgl. Ziff. 8.7). Darin wird u. a. gefordert, dass für jede Datei in einer Errichtungsanordnung der Zweck der Datei und die Speichervoraussetzungen festgelegt werden müssen. Weiterhin wird für alle Verbunddateien eine lückenlose Dokumentation und insbesondere eine gründlich dokumentierte Prognoseentscheidung gefordert. Zudem wird festgestellt, dass die Speicherung von Bagatellfällen in großen Verbunddateien unverhältnismäßig ist. Schließlich ist sicherzustellen, dass vor einer Übernahme des Datenbestandes aus Falldateien im Rahmen des zukünftigen Polizeilichen Informations- und Analyseverbundes (PIAV) die Rechtmäßigkeit der einzelnen Speicherungen überprüft wird.

3.1.2
Änderung des Rundfunkbeitragsstaatsvertrages – erneut bundesweiter Meldedatenabgleich

Der vom Hessischen Landtag ratifizierte 19. Rundfunkänderungsstaatsvertrag sieht für 2018 einen weiteren bundesweiten Meldedatenabgleich vor. Dagegen bestehen erhebliche verfassungsrechtliche Bedenken.

Mitte des Jahres hat der Hessische Landtag dem 19. Rundfunkänderungsstaatsvertrag zugestimmt (Gesetz zu dem Neunzehnten Rundfunkänderungsstaatsvertrag und zur Änderung des Gesetzes zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 27.06.2016, GVBl. I S. 94, Art. 1). Der 19. Rundfunkänderungsstaatsvertrag enthält in Art. 4 umfangreiche Änderungen des Rundfunkbeitragsstaatsvertrages. In der im Rahmen des Gesetzgebungsverfahrens vom Hauptausschuss des Hessischen Landtags durchgeführten Anhörung habe ich mich gegen einen erneuten bundesweiten Meldedatenabgleich gewandt.

3.1.2.1
Verbesserungen

Die Änderungen des Rundfunkbeitragsstaatsvertrages, die der 19. Rundfunkänderungsstaatsvertrag in Art. 4 vorsieht, enthalten durchaus einige datenschutzrechtliche Verbesserungen: In § 11 Abs. 4 Satz 2 und 3 RBStV wird der Kreis der öffentlichen Stellen, bei denen die Rundfunkanstalten personenbezogene Daten ohne Kenntnis des Betroffenen erheben dürfen, einschränkend definiert. Während nach der vorherigen Regelung des § 11 Abs. 4 RBStV jede öffentliche Stelle als Datenlieferant in Betracht kam, dürfen die Rundfunkanstalten künftig nur bei solchen öffentlichen Stellen personenbezogene Daten erheben, die zur Übermittlung der Daten einzelner Inhaber von Wohnungen oder Betriebsstätten befugt sind, wozu insbesondere die Meldebehörden, die Handels- und Gewerberegister und die Grundbuchämter gezählt werden. Auch der Kreis der nicht-öffentlichen Stellen, bei denen die Rundfunkanstalten Informationen über Betroffene einholen können, wird eingeschränkt (§ 11 Abs. 4 Satz 4 RBStV). Daten dürfen nur noch bei Adresshändlern und Adressverifizierern und nicht z. B. bei Arbeitgebern, Versandhändlern oder Versicherungen erhoben werden. Ausdrücklich normiert wird nunmehr der Grundsatz der Direkterhebung beim Betroffenen (§ 11 Abs. 4 Satz 5 Nr. 1 RBStV), d. h., die Rundfunkanstalten dürfen Daten bei Dritten, seien es öffentliche oder private Stellen, nur erheben, wenn die Datenerhebung beim Betroffenen erfolglos war oder nicht möglich ist. In § 11 Abs. 7 RBStV wird nunmehr den Betroffenen ein bereichsspezifischer Auskunftsanspruch gewährt. Die Rundfunkanstalten werden verpflichtet, den Beitragsschuldnern auf Verlangen die Herkunft der Daten mitzuteilen. Für die Beitragsschuldner des Hessischen Rundfunks hat diese Regelung freilich nur klarstellende Bedeutung, da sich ein entsprechender Auskunftsanspruch bereits aus der Vorschrift des § 18 Abs. 3 Satz 1 Nr. 3 HDSG ergibt, die gemäß § 3 Abs. 5 HDSG für die nicht journalistisch-redaktionelle Datenverarbeitung des Hessischen Rundfunks gilt.

§ 11 Abs. 4 Satz 1, 2, 3, 4, 5 Nr. 1 und Abs. 7 RBStV

(4) Die zuständige Landesrundfunkanstalt kann für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach diesem Staatsvertrag besteht, personenbezogene Daten bei öffentlichen und nicht-öffentlichen Stellen ohne Kenntnis des Betroffenen erheben, verarbeiten oder nutzen. Öffentliche Stellen im Sinne von Satz 1 sind solche, die zur Übermittlung der Daten einzelner Inhaber von Wohnungen oder Betriebsstätten befugt sind. Dies sind insbesondere Meldebehörden, Handelsregister, Gewerberegister und Grundbuchämter. Nicht-öffentliche Stellen im Sinne von Satz 1 sind Unternehmen des Adresshandels und der Adressverifizierung. Voraussetzung für die Erhebung der Daten nach Satz 1 ist, dass

1. eine vorherige Datenerhebung unmittelbar beim Betroffenen erfolglos war oder nicht möglich ist, ...

...

(7) Auf das datenschutzrechtliche Auskunftsersuchen eines Beitragsschuldners hat die zuständige Landesrundfunkanstalt dem Beitragsschuldner die Stelle mitzuteilen, die ihr die jeweiligen Daten des Beitragsschuldners übermittelt hat.

3.1.2.2
Kritik

Erheblichen verfassungsrechtlichen Einwänden begegnet dagegen der in § 14 Abs. 9a RBStV vorgesehene erneute bundesweite Meldedatenabgleich. Die vorgesehene massenhafte Übermittlung von Meldedaten durch die Einwohnermeldebehörden an die Landesrundfunkanstalten verstößt gegen den Grundsatz der Verhältnismäßigkeit. Der

Meldedatenabgleich greift in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Meldepflichtigen ein.

Ein vollständiger Meldedatenabgleich ist erstmals im Rahmen der Umstellung der Rundfunkfinanzierung vom gerätebezogenen Gebührenmodell auf ein wohnungsbezogenes Beitragsmodell erfolgt. Gestützt auf § 14 Abs. 9 RBStV hat jede Meldebehörde in Deutschland zum Stichtag 03.03.2013 der zuständigen Landesrundfunkanstalt Meldedaten aller volljährigen Personen übermittelt, insgesamt hat der Beitragsservice von ARD, ZDF und Deutschlandradio in Köln rund 70 Millionen Datensätze erhalten. Wegen der großen Datenmenge erfolgte die Übermittlung in vier Tranchen. Die letzte wurde im April 2014 übermittelt.

Bereits diesen Meldedatenabgleich habe ich im Mai 2011 im Gesetzgebungsverfahren zum 15. Rundfunkänderungsstaatsvertrag kritisiert (Ausschussvorlage HAA/18/17 Teil I Stand: 20.05.2011, S. 24, 33). Die unabhängigen Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung vom 11.10.2010 gefordert, auf die beabsichtigte Übermittlung der Adressdaten aller gemeldeten Volljährigen durch die Meldebehörden zu verzichten und stattdessen die Datenübermittlung auf die bereits vorhandenen Übermittlungsbefugnisse nach dem Melderecht zu beschränken (39. Tätigkeitsbericht, Ziff. 9.9).

Begründet wird der beabsichtigte erneute vollständige Meldedatenabgleich damit, dass er ein notwendiges Instrument sei, um das verfassungsrechtliche Gebot der Lastengleichheit zu verwirklichen. Durch eine fortschreitende Erosion der Bestandsdaten werde die Beitragsgerechtigkeit beeinträchtigt. Nach Auszug aus einer Wohnung (z. B. wegen Trennung, Scheidung oder Auflösung einer Wohngemeinschaft) oder nach dem Tod des bisherigen Beitragsschuldners sei nicht bekannt, wer die Wohnung weiterhin innehabe und damit neuer Beitragsschuldner sei. Die Rundfunkanstalten schätzen den so entstehenden jährlichen Verlust im Datenbestand über Beitragspflichtige auf etwa 200.000 Datensätze. Die Annahmen, von denen bei dieser Schätzung ausgegangen wird, sind jedoch fraglich: Es wird vorausgesetzt, dass der neue Wohnungsinhaber seiner gesetzlichen Anzeigepflicht nicht nachkommt. Es wird unterstellt, dass der Beitragsschuldner auszieht, denn sollte dieser in der Wohnung verbleiben, würde der ausziehende neue Schuldner durch die anlassbezogene Meldedatenübermittlung (siehe § 22 der Meldedaten-Übermittlungsverordnung) den Rundfunkanstalten bekannt. Es wird ferner vermutet, dass in die Wohnung kein bereits beim Beitragsservice registrierter Beitragsschuldner einzieht. Die Landesrundfunkanstalten haben bislang keine belastbaren Zahlen als Beleg für die behauptete Bestandsdatenerosion vorgelegt.

In der Begründung zum 19. Rundfunkänderungsstaatsvertrag wird zwar zutreffend darauf hingewiesen, dass die Rechtmäßigkeit des 2013 bis 2014 durchgeführten Meldedatenabgleichs durch den Bayerischen Verfassungsgerichtshof bestätigt wurde (LTDrucks. 19/3276 S. 26). Dabei ging das Gericht jedoch von der Einmaligkeit des Abgleichs und der besonderen Situation im Zusammenhang mit dem Systemwechsel von der Rundfunkgebühr zum wohnungsbezogenen Beitrag aus:

> „§ 14 Abs. 9 RBStV soll es den Landesrundfunkanstalten ermöglichen, die bereits für den früheren Rundfunkgebühreneinzug gespeicherten und gemäß § 14 Abs. 6 Satz 1 RBStV weiter verwendbaren Daten einmalig zum Inkrafttreten des neuen Rundfunkbeitragsmodells mit dem Melderegister abzugleichen und zu vervollständigen, um eine möglichst lückenlose Bestands- und Ersterfassung im privaten Bereich zu erreichen.“
>
> (Bayerischer Verfassungsgerichtshof, Entscheidung vom 15.05.2014, Az. Vf. 8-VII-12; Vf. 24-VII-12, Rdnr. 159)

Der ebenfalls in der Begründung zum 19. Rundfunkänderungsstaatsvertrag (a. a. O. S. 26) zitierte Verfassungsgerichtshof Rheinland-Pfalz hat sich in seinem Urteil vom 13.05.2014 (VGH B 35/12) nicht explizit mit dem Meldedatenabgleich nach § 14 Abs. 9 RBStV befasst, woraus sich schließen lässt, dass er von der Verfassungskonformität der Norm ausgegangen ist.

In der Begründung zum 15. Rundfunkänderungsstaatsvertrag wird die Rechtmäßigkeit des bundesweiten Meldedatenabgleichs nach § 14 Abs. 9 RBStV im Wesentlichen aus der Einmaligkeit des Abgleichs aus Anlass des Modellwechsels hergeleitet (LTDrucks. 18/3887, S. 29 ff).

Der Rundfunkbeitragsstaatsvertrag stellt den Rundfunkanstalten eine Reihe von alternativen Instrumenten zur Ermittlung potenzieller Beitragsschuldner zur Verfügung:

Neben der allgemeinen Anzeigepflicht nach § 8 RBStV das Auskunftsrecht nach § 9 RBStV, die Befugnis zur Erhebung personenbezogener Daten bei öffentlichen und nicht-öffentlichen Stellen ohne Kenntnis des Betroffenen (§ 11 Abs. 4 RBStV), die regelmäßigen Übermittlungen von Meldedaten nach der Meldedaten-Übermittlungsverordnung. Das sollte eigentlich reichen, denn den Rundfunkanstalten werden damit zur angeblichen Sicherung von Beitragsgerechtigkeit Informationsrechte eingeräumt wie keiner anderen öffentlichen Stelle.

Die zur Pflege des Datenbestandes in der Vergangenheit praktizierte Anmietung von Adressen bei kommerziellen Adresshändlern soll zwar wie auch die Vermieterauskunft nach § 9 Abs. 1 Satz 2 und 3 gemäß § 14 Abs. 10 RBStV wegen des erneuten vollständigen Meldedatenabgleichs bis zum 31.12.2020 ausgesetzt werden. Dies ist jedoch keine echte Kompensation für den massenhaften Eingriff durch den Meldedatenabgleich. Zum einen ist bei dem geplanten Meldedatenabgleich zum Stichtag 01.01.2018 keine Notwendigkeit für Mailingaktionen mittels angemieteter Adressen erkennbar, insbesondere wenn man die anderen Instrumente zur Aktualisierung der Bestandsdaten berücksichtigt. Zum anderen soll anscheinend nach dem 31.12.2020 die datenschutzrechtlich fragwürdige Anmietung von Adressen wieder aufgenommen werden.

Es steht zu befürchten, dass der nächste bundesweite Meldedatenabgleich der Einstieg in eine regelmäßige Rasterfahndung nach Beitragsschuldnern werden soll. Darauf deutet zumindest der Hinweis in der Begründung (a. a. O. S. 26) hin, dass die in § 14 Abs. 9a Satz 4 RBStV angeordnete Evaluierung des Abgleichs mit dem Ziel erfolge, eine Entscheidungsgrundlage für eine dauerhafte gesetzliche Verankerung des Meldedatenabgleichs zu erhalten.

§ 14 Abs. 9a und 10 RBStV

(9a) Zur Sicherstellung der Aktualität des Datenbestandes wird zum 1. Januar 2018 ein weiterer Abgleich entsprechend Abs. 9 durchgeführt. Die Meldebehörden übermitteln die Daten bis längstens 31. Dezember 2018. Im Übrigen gelten Absatz 9 Satz 1 bis 4 und § 11 Abs. 6 Satz 2 und 3 entsprechend. Der Abgleich wird nach seiner Durchführung evaluiert. Die Landesrundfunkanstalten stellen den Ländern hierfür die erforderlichen Informationen zur Verfügung.

(10) Die Landesrundfunkanstalten dürfen bis zum 31. Dezember 2020 keine Adressdaten privater Personen ankaufen.

3.2
Sozialwesen

3.2.1
Einsatz von Außendienstmitarbeitern durch eine SGB II-Optionskommune

Ein SGB II-Leistungsträger hat im Rahmen der Ermittlungen, ob Leistungsmissbrauch vorliegt, stets den Grundsatz der Direkterhebung beim Betroffenen zu beachten. Ein Überprüfungsauftrag an den Außendienst muss geeignete, angemessene und präzise Weisungen enthalten und darf nicht der Auslegung durch die Mitarbeiter des Außendienstes überlassen bleiben.

Anlass

Der Bevollmächtigte eines Beschwerdeführers hat sich bei mir über verschiedene Maßnahmen einer Optionskommune bei der Überprüfung der persönlichen und wirtschaftlichen Verhältnisse des Leistungsempfängers beschwert. Ohne dem Betroffenen vorab Gelegenheit zur Aufklärung zu geben, hatte die Optionskommune eine Halterabfrage zu einem Pkw bei der örtlichen Zulassungsstelle sowie eine Anfrage bei einem Gewerbeamt durchgeführt. Schließlich ließ sie den Betroffenen durch einen beauftragten Außendienst an insgesamt 25 Tagen innerhalb von zwei Monaten beobachten.

Rechtliche Bewertung

Bereits vor und dann bei der Beauftragung des Außendienstes zur „Überprüfung der persönlichen und wirtschaftlichen Verhältnisse“, anlässlich eines anonymen Hinweises, missachtete die Optionskommune sozialdatenschutzrechtliche Vorgaben. Der Grundsatz der Direkterhebung beim Betroffenen wurde an mehreren Stellen übergangen, obwohl die Voraussetzungen für eine hiervon abweichende Datenerhebung zum Zeitpunkt der Beauftragung nicht vorlagen.

§ 67a Abs. 1 SGB X

Sozialdaten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden

1. bei den in § 35 des Ersten Buches oder in § 69 Abs. 2 genannten Stellen, wenn
    a) diese zur Übermittlung der Daten an die erhebende Stelle befugt sind,

    b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und
    c) keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden,
2. bei anderen Personen oder Stellen, wenn
    a) eine Rechtsvorschrift die Erhebung bei ihnen zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt oder
    b) aa) die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen oder
        bb) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde
        und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

So wurde eine Halterabfrage zu einem Pkw bei der örtlichen Zulassungsstelle sowie eine Anfrage bei einem Gewerbeamt gestellt, ohne zunächst dem Betroffenen Gelegenheit zu geben selbst zu den klärungsbedürftigen Sachverhalten beizutragen. Die Optionskommune beachtete bei ihrer Vorgehensweise nicht den Vorrang der sozialdatenschutzrechtlichen Vorgaben vor denjenigen des Sozialverwaltungsverfahrens.

§ 37 Satz 3 SGB I

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

Auch bei der Beauftragung des Außendienstes wurden datenschutzrechtliche Vorgaben missachtet.
Die Einrichtung und das Bestehen eines Außendienstes zur Überprüfung, ob ein Leistungsmissbrauch vorliegt, ist zwar nicht zu beanstanden, sondern vielmehr durch Gesetz in § 6 Abs. 1 Satz 2 SGB II intendiert.

§ 6 Abs. 1 SGB II

Träger der Leistungen nach diesem Buch sind:
1. die Bundesagentur für Arbeit (Bundesagentur), soweit Nummer 2 nichts anderes bestimmt,
2. die kreisfreien Städte und Kreise für die Leistungen nach § 16a, das Arbeitslosengeld II und das Sozialgeld, soweit Arbeitslosengeld II und Sozialgeld für den Bedarf für Unterkunft und Heizung geleistet wird, die Leistungen nach § 24 Absatz 3 Satz 1 Nummer 1 und 2 sowie für die Leistungen nach § 28, soweit durch Landesrecht nicht andere Träger bestimmt sind (kommunale Träger).

Zu ihrer Unterstützung können sie Dritte mit der Wahrnehmung von Aufgaben beauftragen; sie sollen einen Außendienst zur Bekämpfung von Leistungsmissbrauch einrichten.

Allerdings bleiben auch bei der Beauftragung Dritter die jeweiligen Mitarbeiter/Innen der Sachbearbeitung „Herr des Verfahrens“. Deshalb sind von dort klare und datenschutzgerechte Anweisungen an den Außendienst zu erteilen, die nicht erst durch dessen Mitarbeiter/Innen ausgelegt und interpretiert werden müssen.

Im vorliegenden Fall wurde allgemein und ohne nähere Konkretisierung die „Überprüfung der Wohnverhältnisse“ in Auftrag gegeben. Dies führte offensichtlich dazu, dass der Außendienst den Umfang der Maßnahme selbst bestimmte und eine unverhältnismäßige und ausgedehnte Beobachtung des Betroffenen an verschiedenen Lokalitäten unterschiedlicher Städte durchführte, die auch die Beobachtung dritter Personen mit einschloss. Die Verstöße gegen den Sozialdatenschutz manifestierten sich insbesondere in der Erhebung von Daten anderer Personen, in der Begehung der Wohnung einer dritten Person sowie insgesamt in der unverhältnismäßigen Dauer und Intensität der Sachverhaltsermittlung. Dadurch wurde der Grundsatz der Erforderlichkeit deutlich missachtet und ggü. den dritten Personen eine unzulässige Datenerhebung ohne Rechtsgrundlage vorgenommen.

Selbstverständlich ist auch der Außendienst bei der Ausführung des Auftrages an die Beachtung gesetzlicher Vorgaben inklusive derjenigen des Sozialdatenschutzes gebunden. Hier wäre vor Auftragserfüllung eine Rückfrage erforderlich gewesen, um überhaupt einen sinnvollen Auftrag zu definieren.

Letztlich waren die Bemühungen des Außendienstes auch nicht von Erfolg gekrönt: Trotz der extrem umfangreichen Tätigkeit des Außendienstes wurden keine leistungsrelevanten Erkenntnisse zu den persönlichen und wirtschaftlichen Verhältnissen des Betroffenen festgestellt.

Konfrontiert mit dem Fall, räumte der behördliche Datenschutzbeauftragte der Optionskommune in einer sehr umfänglichen Stellungnahme eine datenschutzrechtliche Grenzüberschreitung ein. Er bedauerte dies und sah die Vorgehensweise des

Außendienstes zu Recht datenschutzrechtlich beanstandet. Er anerkannte, dass der „unpräzise und jedes Maß vermissen lassende Auftrag“ zur Überprüfung der persönlichen und wirtschaftlichen Verhältnisse kein Auftrag gewesen sei, den ein Außendienstmitarbeiter sachgerecht hätte erfüllen können. Auch der Landrat der Optionskommune räumte mir gegenüber ein, dass der Außendienst auf der Grundlage eines teilweise ungerechtfertigten, übermäßigen und unpräzisen Auftrags gegen Bestimmungen des Sozialdatenschutzes verstoßen habe und er dies ausdrücklich bedauere.

Nach entsprechendem Schreiben des behördlichen Datenschutzbeauftragten wurden die unzulässig erhobenen Daten von den betreffenden Fachbereichen aus den Akten entfernt. Die Leitung der internen SGB II-Stelle setzte zudem die von mir empfohlene Maßnahme, mittels einer Handlungsanleitung / Dienstanweisung künftig sicherzustellen, dass der Sozialdatenschutz (auch) bei Sachverhaltsermittlungen durch den Außendienst stets beachtet wird, ausreichend um.

Unter diesen Umständen konnte ich von einer förmlichen Beanstandung absehen.

3.2.2

Abstimmung mit der Evangelischen Kirche in Deutschland zum Umgang mit erweiterten Führungszeugnissen bei Trägern der öffentlichen Jugendhilfe

Im Hinblick auf den Umgang mit erweiterten Führungszeugnissen bei Trägern der öffentlichen Jugendhilfe sind de lege lata neben- und ehrenamtlich tätige Personen strenger zu behandeln als hauptamtlich tätige Personen.

Der Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland (EKD) wandte sich an mich, um für das Bundesgebiet eine einheitliche Vorgehensweise zur Auslegung des § 72a Abs. 1 SGB VIII und den Umgang mit Verlangen nach Vorlage von erweiterten Führungszeugnissen bei öffentlichen Jugendhilfeträgern zu erreichen. Nach einer von mir initiierten Umfrage innerhalb der Landesbeauftragten für den Datenschutz konnte dieses Ziel erreicht werden.

Der Datenschutzbeauftragte der EKD teilte mir in seiner Anfrage mit, dass die EKD gegenwärtig die Frage diskutiere, ob ein Führungszeugnis lediglich einzusehen und ein Vermerk über den Inhalt für die Personalakte zu fertigen sei oder ob das Führungszeugnis in geeigneter Weise zu den Akten genommen werden dürfe. Hintergrund dieser Diskussion sei § 72a Abs. 1 SGB VIII, der davon spreche, dass sich die Träger der öffentlichen Jugendhilfe das Führungszeugnis vorlegen lassen müssten. Insoweit sei die Frage, ob „vorlegen lassen“ wörtlich auszulegen sei.

Der EKD liege viel daran, bei grundsätzlichen Fragen des staatlichen Datenschutzes eine abgestimmte Meinung mit den staatlichen Datenschutzbeauftragten zu vertreten.

§ 72a Abs. 1 SGB VIII

Die Träger der öffentlichen Jugendhilfe dürfen für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Person beschäftigen oder vermitteln, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 180a, 181a, 182 bis 184g, 184i, 201a Absatz 3, den §§ 225, 232 bis 233a, 234, 235 oder 236 des Strafgesetzbuchs verurteilt worden ist. Zu diesem Zweck sollen sie sich bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30 Absatz 5 und § 30a Absatz 1 des Bundeszentralregistergesetzes vorlegen lassen.

Ich habe daher eine Umfrage initiiert, in der ich die Kolleginnen und Kollegen der anderen Bundesländer gebeten habe, mir mitzuteilen, wie dort im staatlichen Bereich mit Führungszeugnissen in diesem Sachzusammenhang umgegangen werde. In diesem Zusammenhang habe ich auch auf meinen Beitrag „Minderjährigenschutz in Vereinen – zum Umgang mit erweiterten Führungszeugnissen“ im privaten Bereich hingewiesen (43. Tätigkeitsbericht, Ziff. 5.8.2).

In meiner Zusammenfassung der eingegangenen Rückmeldungen meiner Länderkolleginnen und -kollegen und eigenen datenschutzrechtlichen Bewertung habe ich den Sachverhalt wie folgt beurteilt:

Es besteht weitgehender Konsens über die Frage, wie mit erweiterten Führungszeugnissen **bei neben- und ehrenamtlich tätigen Personen** umzugehen ist, nämlich restriktiv. Hier wird in **§ 72a Abs. 5 SGB VIII** eine gleichermaßen eindeutige wie strenge Vorgabe des Gesetzgebers gesehen, die ihrem Wortlaut nach („Einsicht“) keine Kopie eines (erweiterten) Führungszeugnisses zulässt.

§ 72a Abs. 5 SGB VIII

Träger der öffentlichen und freien Jugendhilfe dürfen von den nach den Absätzen 3 und 4 eingesehenen Daten nur den Umstand, dass Einsicht in ein Führungszeugnis genommen wurde, das Datum des Führungszeugnisses und die Information erheben, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist. Die Träger der öffentlichen und freien Jugendhilfe dürfen diese erhobenen Daten nur speichern, verändern und nutzen, soweit dies zum Ausschluss der Personen von der Tätigkeit, die Anlass zu der Einsichtnahme in das Führungszeugnis gewesen ist, erforderlich ist. Die Daten sind vor dem Zugriff Unbefugter zu schützen. Sie sind unverzüglich zu löschen, wenn im Anschluss an die Einsichtnahme keine Tätigkeit nach Absatz 3 Satz 2 oder Absatz 4 Satz 2 wahrgenommen wird. Andernfalls sind die Daten spätestens drei Monate nach der Beendigung einer solchen Tätigkeit zu löschen.

Etwas anders kann sich der Sachverhalt **bei hauptamtlich tätigen Personen** nach **§ 72a Abs. 1 SGB VIII** darstellen. Der Wortlaut dieser Vorschrift spricht im Zusammenhang des Führungszeugnisses bereits von „vorlegen lassen“ und nicht davon, „dass Einsicht (…) genommen wurde“, wie Absatz 5 dies tut. Es finden sich in Absatz 1 aber auch keine näheren Bestimmungen und Vorgaben, wie mit den Führungszeugnissen über das „vorlegen lassen“ hinaus weiter zu verfahren ist.

Wenn wegen Einträgen in diesem Führungszeugnis ein Tätigkeitsausschluss der betroffenen Person (Beschäftigte/-r oder Bewerber/-in) die Folge ist und womöglich ein arbeitsrechtlicher Streit hieraus resultieren kann, so erscheint in diesem Sonderfall eine beschränkte Speicherung der für den Tätigkeitsausschluss erheblichen Gründe geboten – mithin aber nicht des gesamten Führungszeugnisses.

Insgesamt ist jedoch zu bedenken, dass die von § 72a Abs. 1 SGB VIII angesprochenen hauptamtlich tätigen Personen in einem Arbeits- bzw. Dienstverhältnis stehen und der Umgang mit Führungszeugnissen bei dieser Fallgruppe sich nach den einschlägigen Regelungen der jeweiligen Datenschutzgesetze bzw. anderer spezialgesetzlicher Regelungen bestimmt. Jedenfalls handelt es sich hier um personenbezogene Daten der Beschäftigten, also Beschäftigtendaten, die keine Sozialdaten sind und weshalb die Bestimmungen des Sozialdatenschutzes keine Anwendung finden.

Beispielsweise ist in § 34 Abs. 1 des Hessischen Datenschutzgesetzes (oder auch in § 33 Abs. 1 des Thüringischen Datenschutzgesetzes) sinngemäß geregelt, dass der Dienstherr oder Arbeitgeber Daten seiner Beschäftigten nur verarbeiten darf, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist. Dabei hat er die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes auf Angestellte entsprechend anzuwenden bzw. gelten die entsprechenden Vorschriften des Thüringer Beamtengesetzes, es sei denn, tarifvertragliche Regelungen oder besondere Rechtsvorschriften sähen anderes vor.

Nach diesem Ergebnis müsste man davon ausgehen, dass das erweiterte Führungszeugnis des hauptamtlichen Personals beim öffentlichen Jugendhilfeträger Teil der Personalakte wird, da sich der Umgang mit dieser Unterlage nach den Vorschriften im Zusammenhang mit Dienst- und Arbeitsverhältnissen bestimmt. Besonders hinzuweisen ist jedoch auf die Tatsache, dass es zu der Regelung des § 72a SGB VIII eine Vielzahl von Anfragen, Beschwerden und Anregungen bundesweit gegeben hat und weiter gibt. Die Vorschrift steht zur Evaluierung an, und das Bundesministerium für Familie, Senioren, Frauen und Jugend ist bereits mit einer Klarstellung dieser Regelung befasst.

Dieses Ergebnis habe ich namens der Datenschutzbeauftragten der Länder dem Datenschutzbeauftragten der EKD mitgeteilt. Von diesem erreichte mich keine abweichende Stellungnahme, so dass hier von einer bundeseinheitlichen Verwaltungspraxis ausgegangen werden kann. Es bleibt noch abzuwarten, inwieweit der Gesetzgeber Änderungen am Normtext vornimmt und dann ggf. eine andere Rechtsauffassung zu vertreten sein wird.

3.2.3

Datenaustausch zwischen Jobcenter und Finanzamt

Um Sozialleistungsbetrug aufzudecken, ist es datenschutzrechtlich zulässig, wenn auf Ersuchen des Jobcenters das Finanzamt erforderliche Informationen über die finanziellen Verhältnisse des Sozialleistungsempfängers übermittelt.

Anlass

Ein Jobcenter bat mich um datenschutzrechtliche Beratung mit Blick auf folgenden Sachverhalt:
Das Jobcenter benötige Einkommensnachweise von einem Mitglied einer Hausgemeinschaft (Bedarfsgemeinschaft), da beabsichtigt war, Geldleistungen zurückzufordern. Es sei dem Jobcenter aber nicht näher bekannt, wie der Leistungsempfänger seinen Lebensunterhalt

bestreite. Deshalb sei er persönlich angeschrieben und aufgefordert worden, seine Einkommensnachweise vorzulegen.

Vor diesem Hintergrund wollte das Jobcenter einen datenschutzrechtlichen Hinweis, wie zulässigerweise verfahren werden kann, falls der Leistungsempfänger sich weigert, Einkommensnachweise vorzulegen: Darf dann Auskunft beim Finanzamt eingeholt werden?

Nach vorläufiger Einschätzung des Jobcenters war eine Strafanzeige wegen Sozialleistungsbetrugs als weiteres Vorgehen geplant.

Rechtliche Bewertung

Wenn ein Jobcenter um personenbezogene Auskünfte bei einem Finanzamt ersucht, wird diesem bekannt, dass die betreffende Person in einem Sozialrechtsverhältnis zum Jobcenter steht und insoweit dann auch eine Übermittlung von Sozialdaten vorliegt, die einer gesetzlichen Grundlage bedarf.

Zu den Aufgaben des Jobcenters gehört u. a. unberechtigten Leistungsbezug zu vermeiden und gegebenenfalls auch auf eine strafgerichtliche Ahndung hinzuwirken. Eine damit zusammenhängende Datenübermittlung wird vom Sozialdatenschutzrecht gedeckt (§ 69 Abs. 1 Nr. 1 und Nr. 2 SGB X).

> § 69 Abs. 1 SGB X
>
> Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist
> 1. für die Erfüllung einer gesetzlichen Aufgabe der übermittelnden Stelle nach diesem Gesetzbuch ...
> 2. für die Durchführung eines mit der Erfüllung einer Aufgabe nach Nummer 1 zusammenhängenden gerichtlichen Verfahrens einschließlich eines Strafverfahrens ...

Soweit ein Jobcenter im Rahmen seiner Aufgabenwahrnehmung ein Finanzamt um personenbezogene Daten ersucht und von diesem übermittelt bekommt, liegt eine Datenerhebung nicht beim Betroffenen, sondern bei einer anderen Stelle vor. Gerade die Datenerhebung beim Betroffenen ist aber ein zentrales Prinzip des Datenschutzrechts, das freilich auch seine Schranken hat. Im Sozialdatenschutz ist dieses Prinzip und seine Begrenzungen ausführlich und ausdifferenziert in § 67a SGB X niedergelegt. Knapp formuliert ist eine Datenerhebung eines Jobcenters bei einem Finanzamt zulässig, wenn die Datenerhebung des Jobcenters beim Betroffenen scheitert, etwa weil dieser sich weigert, seinen sozialrechtlichen Mitwirkungsobliegenheiten nachzukommen (§§ 60 ff. SGB I).

Übermittelt ein Finanzamt in einer solchen Konstellation dem Jobcenter die für dessen weiteres Vorgehen erforderlichen Informationen, benötigt das Finanzamt seinerseits eine gesetzliche Befugnis. Diese Übermittlungsbefugnis eines Finanzamtes an die Sozialverwaltung ist an etwas „versteckter“ Stelle gesetzlich geregelt: nämlich weder in der Abgabenordnung noch im Sozialdatenschutzrecht, sondern in § 21 Abs. 4 SGB X, also im Kapitel Verwaltungsverfahren. Diese „Beweismittel“ betreffende Vorschrift verpflichtet die Finanzverwaltung, den Sozialbehörden die für deren Aufgabenwahrnehmung erforderlichen personenbezogenen Auskünfte zu übermitteln.

> § 21 Abs. 4 SGB X
>
> Die Finanzbehörden haben, soweit es im Verfahren nach diesem Gesetzbuch erforderlich ist, Auskunft über die ihnen bekannten Einkommens- oder Vermögensverhältnisse des Antragstellers, Leistungsempfängers, Erstattungspflichtigen, Unterhaltsverpflichteten, Unterhaltsberechtigten oder der zum Haushalt rechnenden Familienmitglieder zu erteilen.

Über diese Rechtslage habe ich das Jobcenter informiert.

3.3
Kommunen und Kammern

3.3.1
Melderecht in der Praxis

Das am 01.11.2015 in Kraft getretene Bundesmeldegesetz hat u. a. das Hessische Meldegesetz ersetzt. Zwar ähnelt die Grundstruktur des Bundesmeldegesetzes den landesrechtlichen Vorgängergesetzen, allerdings sind manche Details, die auch aus datenschutzrechtlicher Sicht Relevanz haben, anders geregelt. Dies führte zu zahlreichen Anfragen an meine Dienststelle. Die häufigsten sollen in diesem Beitrag aufgegriffen werden.

3.3.1.1

Meldedaten an Ortsbeiräte

Verschiedene Kommunen fragten an, ob es statthaft sei, regelmäßig die Einwohnermeldedaten neu hinzugezogener Mitbürger den Ortsbeiräten zur Verfügung zu stellen. Die Ortsbeiräte wollten die neuen Mitbürger mit einem Begrüßungsschreiben über ihren neuen Wohnort informieren.

Die Ortsvorsteher sind öffentliche Stellen i. S. d. Bundesmeldegesetzes, so dass ihnen auch Meldedaten für ihre Aufgabenerfüllung zur Verfügung gestellt werden können. Allerdings bin ich der Auffassung, dass ihnen diese Daten jeweils nur für eine konkrete Aufgabe weitergegeben werden dürfen und die Daten für diese Aufgabenerfüllung auch erforderlich sein müssen.

Das Ziel, Neubürger zu begrüßen oder zu informieren, lässt sich auch ohne eine zusätzliche Datenweitergabe erreichen, indem man beispielsweise einen Flyer im Rahmen der melderechtlichen Anmeldung aushändigt oder sich bei dieser Gelegenheit zweckgebundene Einverständniserklärungen für die Datenweitergabe an die Ortsbeiräte einholt.

Ein Erfordernis zur Datenweitergabe sehe ich vor dem Hintergrund von Alternativen als nicht gegeben, weswegen ich die regelmäßige Weitergabe der Meldedaten zu diesem Zweck untersagt habe.

3.3.1.2

Meldedaten an politische Parteien

Vor dem Hintergrund der hessischen Kommunalwahlen und zahlreicher Bürgermeisterwahlen in Hessen wurde bei mir mehrfach die unaufgeforderte, adressierte Zusendung von Wahlwerbungsmaterial durch die Parteien und die damit einhergehende Übermittlung von Meldedaten moniert.

Das Bundesmeldegesetz sieht in § 50 Abs. 1 BMG eine Übermittlung von Wählerdaten aus dem Melderegister an Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene vor. Übermittelt werden dürfen Daten von Gruppen von Wahlberechtigten, für deren Zusammensetzung das Lebensalter bestimmend ist. So können beispielsweise die Daten der 18- bis 24-Jährigen (Erstwähler) übermittelt werden. In einer Kommune hatte eine politische Partei im Zusammenhang mit der Kommunalwahl die Daten aller erstmals in dieser Kommune Wahlberechtigten erbeten und damit auch die Daten der in die Kommune zugezogenen Bürger begehrt und erhalten. Dies war eine unzulässige Datenübermittlung, weil sich die Zusammensetzung der Gruppe nicht mehr ausschließlich an der Zugehörigkeit zu einer bestimmten Altersgruppe orientierte.

Übermittelt werden dürfen nur Familien- und Vornamen, Doktorgrad, Geschlecht, Staatsangehörigkeiten, derzeitige Anschriften sowie gesetzliche Vertreter mit Familien- und Vornamen sowie Anschrift. Eine Übermittlung des Geburtsdatums der Personen ist nicht zulässig. Diese Daten dürfen innerhalb einer Frist von sechs Monaten vor den Wahlen allein zum Zweck der Wahlwerbung übermittelt werden.

Sofern die adressierte Zusendung von Wahlwerbung im zulässigen Zeitfenster vor Wahlen in Bund, Land oder Kommunen oder anlässlich von Bürgermeisterwahlen erfolgt und sich auf die zulässigen Daten beschränkt, ist sie rechtlich nicht zu beanstanden.

Bürger, die die unaufgeforderte Zusendung von Wahlwerbematerial nicht wünschen, können gemäß § 50 Abs. 5 BMG einer Datenübermittlung widersprechen.

3.3.1.3

Datenübermittlungen im Zusammenhang mit Alters- und Ehejubiläen

Verschiedene Anfragen hatten die Übermittlung von Geburtsdaten und Ehejubiläumsdaten durch die Meldebehörden an die Presse sowie Mandatsträger wie beispielsweise Bürgermeister oder Abgeordnete zum Gegenstand. Die Anfragen kamen sowohl von Bürgern, deren Daten weitergegeben worden waren, als auch von Kommunen, die sich unsicher waren, wann sie die Daten weitergeben dürfen.

In § 50 Abs. 2 BMG sind die Voraussetzungen für eine Datenübermittlung sowohl an die Presse als auch an Mandatsträger formuliert. Anders als die alte Vorschrift im Hessischen Meldegesetz benennt die neue Norm die Anlässe, zu denen eine Datenübermittlung stattfinden darf.

§ 50 Abs. 2 Satz 2 BMG

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Übermittelt werden lediglich Familien- und Vornamen, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums.

Auch dieser Datenübermittlung können die Betroffenen gemäß § 50 Abs. 5 BMG widersprechen. Über dieses Widerspruchsrecht sind sie bei der Anmeldung und mindestens einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen.

Formulare zu den Widersprüchen stehen auf meiner Homepage (www.datenschutz.hessen.de).

3.3.1.4

Auskunftssperren

Einige Kommunen wollten wissen, wie bei Auskunftsersuchen zu verfahren ist, wenn eine Auskunftssperre nach § 51 BMG für die betroffene Person eingetragen ist.

Die Regelungen zum Umgang mit Melderegisterauskünften bei Vorliegen einer Auskunftssperre wegen der Bedrohung von Leib und Leben haben sich durch die Einführung des Bundesmeldegesetzes geändert. Die nun normierten und praktizierten Abläufe zur Beauskunftung gesperrter Daten stärken den Schutz derer, die durch die Offenbarung ihrer Meldedaten Gefährdungen ausgesetzt wären. Entgegen der alten Regelung im Hessischen Meldegesetz ist die Person, deren Daten gesperrt sind, in den Prozess zu einer möglichen Auskunftserteilung im Einzelfall mit einbezogen, indem sie zu der gewünschten Auskunft angehört wird. Im Anschluss an die Anhörung trifft die Meldebehörde eine Entscheidung, ob sie die Auskunft erteilt oder nicht. Kann nicht ausgeschlossen werden, dass durch die Auskunft eine Gefährdung für die betroffene Person entstehen würde, darf keine Auskunft erteilt werden. Dabei regelt § 51 BMG jetzt unmissverständlich, dass die Auskunft nicht erkennen lassen darf, ob zu der betroffenen Person keine Daten vorhanden sind oder eine Auskunftssperre besteht.

Da für die erforderliche Anhörung eine Frist von zwei Wochen einzuräumen ist, verzögert sich das Auskunftsverfahren seit dem Inkrafttreten des Bundesmeldegesetzes nicht unerheblich.

3.3.1.5

Mitwirkung des Wohnungsgebers bei der Anmeldung

Zahlreiche Wohnungsgeber, also Vermieter, meldeten sich bei meiner Dienststelle und hinterfragten die Regelung des § 19 BMG.

Die alte Regelung in § 14 HMG sah bereits die Möglichkeit vor, dass die Meldebehörden ein Auskunftsrecht gegenüber dem Wohnungsgeber oder der Wohnungsgeberin geltend machten, wenn diese die Wohnungsbelegung im Rahmen ihrer Aufgabenerfüllung verifizieren wollten. Ein generelles Mitwirken des Wohnungsgebers fand damit allerdings nicht statt.

Die jetzt gültige Norm des § 19 BMG normiert demgegenüber eine Mitwirkungspflicht des Wohnungsgebers oder der Wohnungsgeberin beim Meldevorgang. Dies hat zur Folge, dass auch die Wohnungsgeber personenbezogene Daten im Zusammenhang mit der Anmeldung von Mietern offenbaren müssen. Dies wurde von manchen kritisch hinterfragt.

Nachdem zunächst auch eine Mitwirkungspflicht beim Abmeldevorgang, d. h. beim Wegzug des Mieters, vorgeschrieben war, wurde die Vorschrift des § 19 Abs. 1 BMG zum 01.11.2016 dahingehend geändert, dass sich die Mitwirkungspflicht nunmehr ausschließlich auf die Anmeldung bezieht. Eine Mitwirkungspflicht bei der Abmeldung besteht nicht mehr.

3.3.2

Amtshilfe und Datenschutz

Beabsichtigt eine Architektenkammer, gegen einen Architekten ein Ordnungswidrigkeitenverfahren einzuleiten, ist es rechtlich fehlerhaft, ihr Auskunftsersuchen gegenüber der Bauaufsicht auf das Amtshilfeprinzip zu stützen.

Anlass

Die Bauaufsichtsbehörde eines Landkreises fragte bei mir an, ob es zulässig sei, personenbezogene Informationen über einen Architekten an eine Architektenkammer zu übermitteln. Diese wolle gegen besagten Architekten ein Ordnungswidrigkeitenverfahren einleiten und habe ihr Informationsbegehren mit dem Hinweis auf das Amtshilfeprinzip gerechtfertigt.

Rechtliche Bewertung

Dass sich die Behörden des Bundes und der Länder gegenseitig Amtshilfe leisten, ist ein verfassungsrechtliches Prinzip.

> Art. 35 Abs. 1 GG
>
> Alle Behörden des Bundes und der Länder leisten sich gegenseitig Rechts- und Amtshilfe.

Diese verfassungsrechtliche Vorgabe hat einfachrechtlich in den Verwaltungsverfahrensgesetzen des Bundes und der Länder ihre nähere Ausgestaltung bekommen. In Hessen ist bspw. der Amtshilfegrundsatz in den §§ 4 ff. HVwVfG näher geregelt und insbesondere vorgeschrieben, dass jede Behörde anderen Behörden auf Ersuchen ergänzende Hilfe leistet (§ 4 Abs.1 HVwVfG).

Da aber nicht nur die Amtshilfe, sondern auch das Recht auf informationelle Selbstbestimmung eine verfassungsrechtliche Verankerung hat (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG), könnte immer dann ein Rechtsproblem entstehen, wenn es bei der Amtshilfe zugleich um personenbezogene Daten geht. Der Gesetzgeber hat dieses Problem dadurch entschärft, dass er in diesem Fall dem Datenschutzrecht gegenüber dem Amtshilferecht den Vorrang eingeräumt hat.

> § 3 Abs. 2 HDSG
>
> Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

Die das Amtshilferecht derogierende Wirkung des Datenschutzrechts lässt sich freilich verfassungsrechtlich nur dann rechtfertigen, wenn zugleich das Verfassungsprinzip Amtshilfe hinreichend berücksichtigt wird. Ganz dementsprechend hat der Gesetzgeber dafür Sorge getragen, dass etwa bei der Verfolgung von Ordnungswidrigkeiten das Datenschutzrecht nicht als unüberwindbare Hürde den Weg versperrt. Rechtstechnisch ist dies dadurch erfolgt, dass der Gesetzgeber die Nutzung von Daten zwecks Verfolgung von Ordnungswidrigkeiten als erlaubte Durchbrechung des Gebots der Zweckbindung im Datenschutzrecht ausgestaltet hat; § 13 Abs. 2 i. V. m. § 12 Abs. 2 Nr. 4 HDSG.

> § 13 Abs. 2 HDSG
>
> Sollen personenbezogene Daten zu Zwecken verarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, dann ist dies nur aus den in § 12 Abs. 2 und 3 genannten Gründen zulässig.
>
> § 12 Abs. 2 Nr. 4 HDSG
> ...
> 4. sich ... Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben ...

Vor diesem Hintergrund konnte ich der Bauaufsicht mitteilen, dass der Hinweis der Architektenkammer auf das Amtshilfeprinzip bei personenbezogenen Daten zwar nicht rechtlich korrekt ist, dass aber auch das vorrangige Datenschutzrecht der Übermittlung personenbezogener Daten zwecks Durchführung eines Ordnungswidrigkeitenverfahrens nicht entgegensteht.

3.4
Schulen und Hochschulen

3.4.1
Das Recht am eigenen Bild: Wie müssen Schulen mit diesem Thema gegenüber Eltern umgehen?

Auch wenn das Recht am eigenen Bild als Ausfluss des allgemeinen Persönlichkeitsrechts einen hohen Stellenwert einnimmt, ist dessen Durchsetzung im schulischen Bereich *gegenüber den Eltern praktisch kaum möglich. Die Schule hat jedoch die Pflicht, für eine Sensibilisierung zu sorgen, wenn Eltern bei schulischen Veranstaltungen fotografieren.*

Dass nach Kunsturhebergesetz (KunstUrhG) die schriftliche Einwilligung der Betroffenen oder deren Eltern erforderlich ist und die Einwilligung eine differenzierte Abstufung hinsichtlich des Veröffentlichungszwecks beinhalten muss, hat sich an Schulen allenthalben etabliert.

> § 22 KunstUrhG
>
> Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten.

Im Berichtszeitraum hat mich die sich daran anschließende Frage, wie die Schule mit den widerstreitenden Ansichten und Verhaltensweisen anderer Eltern zur Frage des Fotografierens und der Veröffentlichung von Fotografien ihrer Kinder bei einer gemeinsamen schulischen Veranstaltung umzugehen hat, intensiv beschäftigt.

3.4.1.1
Die Beschwerde eines Elternpaares

Die Eltern von drei schulpflichtigen Kindern beschwerten sich bei mir darüber, dass bei schulischen Veranstaltungen immer wieder Eltern anderer Kinder nicht nur die eigenen Sprösslinge, sondern auch die Kinder der Beschwerdeführer fotografierten. Sie erwarteten von der Schule, dies zu unterbinden, und beriefen sich dabei auf das Recht ihrer Kinder am eigenen Bild. Außerdem, so argumentierten sie, könne die Schule auch ein Verbot zum Anfertigen von Bildern erlassen bzw. dies nur in besonders ausgewiesenen Zonen auf dem Schulgelände zulassen. Hinsichtlich der Durchsetzung eines solchen Verbotes beriefen sich die Beschwerdeführer auf das Hausrecht der Schule, welches diese nur durchsetzen müsse. Die Schule habe den berechtigten Anspruch auf das Recht am eigenen Bild eines jeden Kindes zu respektieren und in aller Konsequenz auch durchzusetzen.

3.4.1.2
Kontaktaufnahme mit Staatlichem Schulamt und Ministerium

In Anbetracht der grundsätzlichen Bedeutung der Thematik nahm mein Mitarbeiter mit dem zuständigen Staatlichen Schulamt (SSA) Kontakt auf und schaltete zudem die Datenschutzbeauftragte des Hessischen Kultusministeriums (HKM) ein. Dabei war man sich bewusst, dass die Rechtsprechung der unterinstanzlichen Gerichte dem allgemeinen Persönlichkeitsrecht der Betroffenen oftmals eine übergeordnete Bedeutung eingeräumt hat, so z. B. Landgericht Münster, Az. 10 O 626/03 vom 24.03.2004 oder Landgericht Frankfurt/Main vom 19.01.2006 (Az.: 2/03 O 468/05), während der Bundesgerichtshof (BGH) mit Urteil vom 08.04.2014 (Az. VI ZR 197/13) entschieden hat, dass das Recht am eigenen Bild hinter der Meinungs- und Pressefreiheit zurückzutreten habe.

Bei einem gemeinsamen Treffen in meiner Dienststelle wurden die inhaltlichen Aspekte des Begehrens der Petenten sowie die Frage nach einer praktikablen und tragfähigen Umsetzung durch die Schulen diskutiert.

3.4.1.3
Bewertung des Sachverhalts

Um es vorwegzunehmen: Eine Lösung, wie sie den Eltern vorschwebte, wonach die Schule im Zweifel exekutiv gegen Eltern vorgehen sollte, die das Fotografierverbot missachten, konnte von den zuständigen Behörden nicht mitgetragen werden.

Einvernehmlich festgestellt wurde, dass es Aufgabe der Schule ist, die rechtlichen Vorgaben der §§ 22 ff. KunstUrhG im Rahmen des eigenen Handelns zu beachten. Dies erfolgt in der Regel durch Einwilligungserklärungen der Eltern für die Fertigung und Verbreitung von Bildern bei Veranstaltungen der Schule.

Ebenso kann von der Schule erwartet werden, für das Thema zu sensibilisieren und Rücksichtnahme bei den Eltern einzufordern. Im Rahmen der Fürsorgepflicht ist die Schule allerdings gehalten, offensichtlich rechtswidrige, den §§ 22 ff. KunstUrhG erkennbar zuwiderlaufende Handlungen durch entsprechende Maßnahmen (z. B. der Ausübung des Hausrechts) entgegenzuwirken. Denkbar sind hier Fälle, in denen ein Kind gegen seinen Willen oder den der Eltern von anderen Eltern im Porträt fotografiert wird und umstehende Lehrkräfte dies ohne Zweifel zur Kenntnis nehmen. Einfluss nehmen kann Schule auch im

Rahmen von Elternbriefen, um vor öffentlichen Schulveranstaltungen auf rechtliche Rahmenbedingungen hinzuweisen und alle Akteure für einen verantwortungsbewussten Umgang mit Medien zu sensibilisieren.

Eine stringente Ausübung des Hausrechts, um z. B. bei Zuwiderhandlungen gegen Eltern tätig werden zu können, wäre der Schule rechtlich durchaus möglich. In seiner faktischen Ausübung aber erscheint dies nicht realistisch zu sein. Hier muss der Betroffene selbst im konkreten Einzelfall straf- oder zivilrechtliche Schritte gegen diejenigen einleiten, die aufgestellte bzw. vereinbarte Regelungen augenscheinlich missachten.

3.4.1.4
Fazit

Eine Schule hat Fürsorgepflichten gegenüber jenen, die das Fotografiertwerden bei schulischen Veranstaltungen durch Dritte ablehnen. Sie kann Verhaltenshinweise geben und deren Beachtung einfordern. Im Konfliktfall ist es jedoch bei einer derartigen Fallkonstellation der Schule aus praktischen Erwägungen nicht möglich, ihr Hausrecht in Form von Hausverboten, der Einziehung von Smartphones und Fotoapparaten oder anderen repressiven Handlungen durchzusetzen.

3.4.2
Datenschutzrechtliche Aspekte bei der Führung von Schülerakten

Im Berichtsjahr haben mich ungewöhnlich viele Eingaben von Eltern erreicht, die Beschwerden im Zusammenhang mit der Führung bzw. dem Inhalt von Schülerakten ihrer Kinder äußerten.

Das Hessische Schulgesetz (HSchulG) regelt, dass eine Schülerakte zu führen ist und was diese zu enthalten hat.

§ 83 Abs. 1 Satz 2 HSchulG

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

§ 1 Abs. 3 Verordnung über die Verarbeitung personenbezogener Daten in Schulen

Schulen führen Schulakten (Vorgänge der allgemeinen Verwaltung der Schule) und legen für jede Schülerin und jeden Schüler eine Schülerdatei an, in der die personenbezogenen Daten gespeichert werden. Die Schülerdatei kann in elektronischer Form (LUSD) und in Papierform (Schülerakte mit Schülerkarte) geführt werden. Die Schülerkarte kann durch den jeweils aktuellen Ausdruck des Stammdatenblatts und der Dokumentation des Bildungsgangs aus der LUSD ersetzt werden.

3.4.2.1
Was in eine Schülerakte aufzunehmen ist

In eine Schülerakte aufzunehmen sind die Grunddaten der Schülerin oder des Schülers, wie sie in der Anlage 1 der Verordnung zur Verarbeitung personenbezogener Daten an Schulen enthalten sind. Hinzu kommen die Organisations- und Schullaufbahndaten sowie Leistungsdaten, wie z. B. Zeugnisnoten, Versetzungsentscheidungen, Ergebnisse von Prüfungen. Schließlich sind noch schulartspezifische Zusatzdaten zu erfassen. Dabei handelt es sich um Informationen, welche speziell für die Grundschule, die Sekundarstufen I und II, die Berufsschulen oder die Förderschulen über die Betroffenen erhoben werden. Auch getroffene Ordnungsmaßnahmen sind in die Schülerakte aufzunehmen und am Ende des zweiten Schuljahres nach der Eintragung zu löschen, sofern nicht während dieser Zeit eine erneute Ordnungsmaßnahme getroffen wurde (§ 82 Abs. 10 HSchulG).

Im Übrigen gilt:
In die Schülerakte sind alle Informationen aufzunehmen, welche für die Schullaufbahn einer Schülerin bzw. eines Schülers von Bedeutung sind. Bei der Auslegung, was nun im Einzelnen von Bedeutung sein kann, kommt es immer wieder zu Fehlinterpretationen. So wurde in einem Fall durch eine Klassenlehrerin in einer Grundschule schriftlich festgehalten, dass eine Schülerin über die Schlafgewohnheiten der Familie berichtet habe. Eine derartige Information hat nichts in einer Schülerakte und auch nichts in anderen schulischen Unterlagen zu suchen.

In einem anderen Fall nahm die Schule einen umfangreichen Fragebogen eines minderjährigen Schülers zur Akte, den die Klassenlehrerin auf Bitten einer psychologischen Ambulanz ausgefüllt hatte. Darin wurden u. a. ihre persönlichen Einschätzungen zu dem Schüler erfragt. Viele dieser Schilderungen waren persönlich „gefärbt“. Weder der Schüler noch seine Eltern waren über den Vorgang informiert. Erst bei der Einsicht in die Schülerakte erfuhren die Eltern, dass das Papier zum Bestandteil der Schülerakte gemacht worden war. Eine derartige Verfahrensweise der Schule bzw. der Lehrkraft ist unzulässig. Als Teil der Dokumentation der Schullaufbahn des Betroffenen waren diese Informationen nicht erforderlich, es mangelte also an der Rechtsgrundlage für die Speicherung der Daten. Auch eine rechtfertigende Einwilligung der Eltern lag nicht vor.

3.4.2.2
Informationsrechte der Schüler und Erziehungsberechtigten

§ 72 Abs. 4 HSchulG

Die Eltern volljähriger Schülerinnen und Schüler sind bis zur Vollendung des 21. Lebensjahres über wesentliche das Schulverhältnis betreffende Sachverhalte, insbesondere über Versetzungsgefährdungen und Nichtversetzungen, über Ordnungsmaßnahmen nach § 82 Abs. 2 Satz 1 Nr. 5 bis 7 und Abs. 8 und gegebenenfalls deren Anordnung sowie über Maßnahmen nach § 82a zu informieren, sofern die volljährige Schülerin oder der volljährige Schüler dem nicht widersprochen hat. Über den Widerspruch werden die Eltern von der Schule informiert. Die Schülerinnen und Schüler sind auf diese Regelung hinzuweisen.

Bürgerinnen und Bürger haben einen Anspruch darauf, zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“. Das verlangt das Bundesverfassungsgericht im Volkszählungsurteil von 1983 (BVerGE 65, 1, 43). Das ist fraglos nur möglich, wenn sie von der Behörde Auskunft hinsichtlich der über sie gespeicherten Daten verlangen oder – noch besser – Einsicht in die einschlägigen Akten nehmen können. Geht es um eine konkrete Verwaltungsentscheidung, also beispielsweise um eine Versetzung, gewährt § 29 HVwVfG den Betroffenen ein Akteneinsichtsrecht. § 72 Abs. 5 HSchulG präzisiert dieses allgemeine Verfahrensrecht.

§ 72 Abs. 5 HSchulG

Jugendliche, die Eltern und volljährige Schülerinnen und Schüler haben das Recht, Akten der Schule, Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter derart verbunden sind, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist den Betroffenen über die zu ihrer Person gespeicherten Daten Auskunft zu erteilen.

§ 72 Abs. 5 HSchulG ist auf Fälle anzuwenden, in denen Eltern, Schülerinnen und Schüler auch außerhalb eines Verwaltungsverfahrens Unterlagen, welche Daten über sie enthalten, einsehen wollen. Dem HDSG ließe sich zwar für diese Fälle ebenfalls ein Akteneinsichtsrecht entnehmen (§ 18 Abs. 4), die Vorschrift ist allerdings nicht so eindeutig formuliert. Deswegen ist streitig, ob die Behörde nicht eine Wahlmöglichkeit zwischen der Gewährung der Akteneinsicht und der Erteilung einer Auskunft hat. Das Schulgesetz trifft hier eine klare Regelung im Sinne eines umfassenden Informationsanspruches: Eltern und Schülerinnen und Schüler haben das Recht, Akten der Schule, der Schulaufsichtsbehörden und des schulärztlichen Dienstes, in denen Daten über sie gespeichert sind, einzusehen. Dieses Recht können auch Schülerinnen und Schüler unter 18 Jahren ausüben. Von besonderer Bedeutung ist grundsätzlich, dass das Einsichtsrecht fast vorbehaltlos gesetzlich anerkannt ist. Eine Einschränkung gibt es allerdings, wie wir sie auch aus dem HDSG (§ 18 Abs. 5) kennen: Sind die Daten der Betroffenen mit Angaben Dritter derart verbunden, dass die Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, ist die Einsichtnahme unzulässig. In diesem Fall ist die Schule jedoch zur Auskunft verpflichtet.

3.4.3
Modernes Bildungsmanagement in der Schule

Bereits seit Jahren wird das Produkt „Edunite“ von einer Reihe hessischer Schulen genutzt. Das Hessische Kultusministerium hatte die Nutzung des Produkts zunächst an ausgewählten hessischen Schulen im Wege eines Pilotprojekts gefördert. Die Beteiligung meiner Behörde war von Anfang an sichergestellt. Nunmehr soll „Edunite“ auch von den Frankfurter Beratungs- und Förderzentren (BFZ) eingesetzt werden. Da dort besonders sensitive Daten, u. a. Gesundheitsdaten, verarbeitet werden, haben die Schulen der BFZ im besonderen Maße auf eine datenschutzkonforme Umsetzung zu achten.

3.4.3.1
„Edunite“ – eine webbasierte Cloud-Lösung

Bereits in der Pilotphase des Einsatzes von „Edunite“ kam ich zu einer grundsätzlich positiven Bewertung der Anwendung. Mit der Software können z. B. virtuelle Klassenkonferenzen durchgeführt, Unterrichts- und Vertretungspläne erstellt und Lernziele etabliert werden. Es beinhaltet zudem eine Kommunikationsplattform, mittels derer Lehrer, Schüler und Eltern mit- und untereinander kommunizieren können. Hierfür sind nutzerbezogene Portale eingerichtet.

Ausschlaggebend für eine positive Bewertung war seinerzeit die doppelte Verschlüsselung der Daten mit einem anwender- und einem schulbezogenen Schlüssel, einer Ende-zu-Ende-Verschlüsselung beim Datentransport sowie dem detaillierten und schlüssigen Rollen- und Berechtigungskonzept. Die Verwaltung der Daten erfolgt in der sog. „Edunite Secure-Cloud“ in einem Rechenzentrum in Frankfurt am Main.

3.4.3.2
Nutzung von „Edunite“ durch die Frankfurter BFZ-Schulen

Im Berichtsjahr sind die fünf schulischen Beratungs- und Förderzentren (BFZ) in Frankfurt mit der Bitte an mich herangetreten, die datenschutzrechtlichen Anforderungen an den Aufbau und den Betrieb einer webbasierten Plattformlösung – gewünscht war der Einsatz von „Edunite“ – zu formulieren. Dabei war zu berücksichtigen, dass gerade in diesem Bereich der Schulverwaltung eine Fülle personenbezogener, medizinischer und sozialer Daten verarbeitet werden. Der Schutzbedarf dieser Daten ist entsprechend hoch und stellt an den Dienstleister, vor allem aber auch an die Anwender hohe Anforderungen im Umgang und der Nutzung von „Edunite“. In diversen Gesprächen mit dem Plattformbetreiber sowie den Schulleitern der BFZ-Schulen habe ich dann Feststellungen getroffen und Anforderungen formuliert, welche an den Einsatz von „Edunite“ unabdingbar geknüpft sind. Dabei handelte es sich weniger um Forderungen gegenüber dem Produktanbieter selbst als gegenüber den Anwendern, also den Schulen. Diese müssen vor Ort sicherstellen, dass Administration, Rollen- und Rechtevergabe sowie mobile Zugriffe den datenschutzrechtlichen Vorgaben entsprechen. Dies erfordert unmittelbar beim Anwender eine konzeptionelle Vorarbeit und Beschreibung eines Anforderungsprofils.

Im Einzelnen habe ich den Schulen Folgendes mitgeteilt:

Auftragsdatenverarbeitung

Der Einsatz der plattformgestützten Anwendung „Edunite“ beinhaltet die Beauftragung des Auftragnehmers, welcher die Plattform technisch und rechtlich betreibt. Der Auftragnehmer verarbeitet personenbezogene Daten von Schülerinnen und Schülern, deren Eltern sowie Lehrkräften der Frankfurter BFZ-Schulen. Nach § 4 Abs. 2 HDSG hat der Auftraggeber (also die Schulen) mit dem Auftragnehmer einen schriftlichen Vertrag abzuschließen, in dem u. a. die Rechte und Pflichten der Parteien sowie der Umfang der Datenverarbeitung geregelt sind. Zudem hat sich der Auftragnehmer gemäß § 4 Abs. 3 HDSG zu verpflichten, im Rahmen des Auftrags die Vorgaben des HDSG zu befolgen und sich meiner Kontrolle zu unterwerfen.

> § 4 HDSG
>
> (2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Zuverlässigkeit und Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen; dabei sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen. ...
>
> (3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. ...

Gemeinsames Verfahren nach § 15 HDSG

Die Frankfurter Förderschulen beabsichtigen, gemeinsam ein Verfahren zu betreiben, welches der Auftragnehmer in Form der plattformbasierten Anwendung „Edunite“ anbietet. Maßgebend für ein gemeinsames Verfahren sind auch die inhaltlich gleichen Parameter, unter denen die Verarbeitung personenbezogener Daten stattfindet. Für jede Art der automatisierten Verarbeitung personenbezogener Daten ist ein Verfahrensverzeichnis zu erstellen.

§ 15 Abs. 1 HDSG

Die Einrichtung eines automatisierten Verfahrens, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. ...

Rollen- und Berechtigungskonzept

Ein derartiges Konzept ist unter datenschutzrechtlichen Gesichtspunkten ein wesentlicher Bestandteil des gesamten Datenverarbeitungskomplexes. Grundsätzliches wird bereits durch „Edunite“ selbst abgebildet bzw. reguliert. Dennoch obliegen den Anwendern selbst vor Ort weitere, wichtige Festlegungen. So ist bei der Ausgestaltung der Zugriffe, die von dienstlichen Rechnern aus auf dem Schulnetz des Schulträgers erfolgen, eine fachliche Bewertung durch den Schulträger erforderlich. Darin soll u. a. enthalten sein, wie und durch wen die Rollen und Berechtigungen der Nutzer festgelegt werden und wer für deren Aktualisierung zuständig ist.

Zugriffe auf „Edunite“ mit privaten bzw. mobilen Endgeräten

Die Zugriffe mit privaten Endgeräten werden zunächst auf das „Live-System“ im Weg einer Stick-Lösung beschränkt. Anderweitige Konfigurationen mit gleichem oder ähnlichem Schutzniveau können in erforderlichem Umfang künftig ggfs. zugelassen werden. Ein mobiler Zugriff durch Smartphones und/oder Tablets bleibt einer landeseinheitlichen Regelung vorbehalten.

Aktivierung einer Textverarbeitung im gekapselten Browser

Der Anbieter von „Edunite“ hat angekündigt, eine derartige Funktionalität in seine Anwendung zu implementieren. Damit könnte eine lokale Speicherung sensitiver, personenbezogener Daten auf privaten Endgeräten technisch wirkungsvoll unterbunden werden. Allerdings setzt dies eine sichere Systembasis voraus, die nur durch ein Device Management realisiert werden kann.

Protokollierung

Hinsichtlich der Anmeldedaten für „Edunite“ ist eine Speicherung von 90 Tagen erforderlich. Nach dem derzeitigen Informationsstand werden in der Datenbank des Auftragnehmers alle Systemaktivitäten von Personen protokolliert, die „Schreibenden Zugriff“ haben. Die Speicherdauer dieser Protokolldateien ist derzeit unbekannt. Für die „Lesenden Zugriffe“ muss der zeitliche und inhaltliche Umfang einer Protokollierung noch geklärt werden. Für Zugriffe, die nicht aus dem Netz des Schulträgers erfolgen, ist ebenfalls eine Protokollierung erforderlich. Aus dieser sollten sich Rückschlüsse auf das verwendete Endgerät ergeben können. Eine virtuelle Kennzeichnung der dabei zur Verwendung kommenden Sticks kann hierbei zielführend sein.

3.4.3.3

Zusammenfassung

Der Einsatz der webbasierten Anwendung „Edunite“ durch die fünf Frankfurter schulischen Beratungs- und Förderzentren (BFZ) ist datenschutzrechtlich dann unproblematisch, soweit die Anwender grundsätzliche Aspekte der Administration im Zusammenhang mit der Rollen- und Rechtevergabe, des Device Managements bei mobilen Endgeräten sowie der Protokollierung umsetzen. Die Unterstützung durch den Softwareanbieter und Dienstleister scheint gewährleistet zu sein. Die Umsetzung des Projekts könnte über die Stadt Frankfurt hinaus auch für andere der insgesamt knapp 140 hessischen BFZ eine Wirkung erzielen. Schließlich ist die datenschutzkonforme Realisierung der Datenverarbeitung in den hessischen BFZ seit Jahren in der Diskussion und bedarf absehbar einer abschließenden Lösung.

4. Datenschutz im nicht-öffentlichen Bereich – Aufsichtsbehörde nach § 38 BDSG

4.1
Vereine

4.1.1
Datenverarbeitung durch einen Sportverband

Die Nutzung eines Videoaufzeichnungssystems durch einen Sportverband zur Kontrolle kampfrichterlicher Entscheidungen ist grundsätzlich zulässig. Eine darüberhinausgehende Nutzung bedarf der ausdrücklichen Einwilligung aller Athleten. Kampfrichterinnen und -richter sind auf das Datengeheimnis nach § 5 BDSG zu verpflichten.

Nutzung eines Videoaufzeichnungssystems durch den Hessischen Judo-Verband e. V.

Der Hessische Judo-Verband e. V. (HJV) nutzte zur Entscheidungsfindung in Zweifelsfällen ein Videoaufzeichnungssystem. Im Rahmen von Wettkämpfen, die der HJV ausrichtet, wurden Videoaufnahmen auf einem eigens hierfür vorgesehenen Laptop gespeichert. Die Aufzeichnung beschränkte sich auf den Wettkampf zwischen den Athleten. Zweck der Aufzeichnungen war es, den Kampfrichtern in Zweifelsfällen durch Ansicht der umstrittenen Kampfsequenz die Möglichkeit der Überprüfung ihrer kampfrichterlichen Entscheidungen zu geben. Die Aufzeichnungen wurden jedoch nach Beendigung des Wettkampfes nicht von dem jeweiligen Laptop gelöscht. Die Aufnahmen wurden stattdessen zu Schulungszwecken weiterverwendet, ohne dass dies den Betroffenen transparent gemacht wurde.

Die Videoaufzeichnung zum Zweck der Überprüfung unklarer Situationen während des Wettkampfes ist durch die Wahrung berechtigter Interessen des HJV gemäß § 28 Abs. 1 Nr. 2 BDSG gedeckt, so dass die Aufzeichnung grundsätzlich zulässig ist. Es liegt auch im Interesse der Athleten, dass durch die Kampfrichter korrekte Entscheidungen getroffen werden. Werden die Aufnahmen unmittelbar nach dem Wettkampf gelöscht, stehen überwiegende Interessen der Athleten einer Aufzeichnung nicht entgegen. Allerdings gilt auch bei zulässigen Aufzeichnungen das Gebot der Transparenz. Die Videoaufzeichnungen der Athleten im Wettkampf dürfen daher nicht ohne entsprechende Hinweise erfolgen. Dies war beim HJV nicht der Fall und musste korrigiert werden.

Die Verwendung der aufgenommenen Videos zu Schulungszwecken kann im Gegensatz zur Überprüfung unsicherer Entscheidungen nicht auf ein berechtigtes Interesse des HJV gemäß § 28 Abs. 1 Nr. 2 BDSG gestützt werden. Hier überwiegt das Interesse der Athleten am Unterbleiben einer entsprechenden Nutzung. Auch eine Einwilligung für die Nutzung lag nicht vor. Diese hätte in Schriftform vorliegen müssen, was nicht der Fall war. Diese Nutzung war daher zu untersagen. Der HJV hat sich im Verlauf des Prüfungsverfahrens verpflichtet, eine derartige Nutzung zu unterlassen und die aufgenommenen Videos unmittelbar nach dem Wettkampf von den jeweiligen Laptops zu löschen.

Verpflichtung der Kampfrichter auf das Datengeheimnis gemäß § 5 BDSG

Eine Überprüfung ergab außerdem, dass die eingesetzten Kampfrichterinnen und -richter nicht vollständig auf das Datengeheimnis nach § 5 BDSG verpflichtet waren.

Die bei den jeweiligen Wettkämpfen des HJV eingesetzten Kampfrichterinnen und -richter haben neben der Beobachtung und Bewertung der Kämpfe die generelle Überprüfung der Starterlaubnis und Identitätskontrolle durch den Judo-Pass oder Personalausweis sowie die Erfassung von Gewicht, Alter etc. vorzunehmen. Damit sind sie mit der Verarbeitung von personenbezogenen Daten befasst und daher auch nach § 5 BDSG auf das Datengeheimnis zu verpflichten. Mangels Verpflichtung aller Kampfrichter auf das Datengeheimnis lag ein Verstoß gegen § 5 Satz 2 BDSG vor. Dem HJV wurde deshalb aufgegeben, die eingesetzten Kampfrichterinnen und -richter sukzessive auf das Datengeheimnis zu verpflichten.

Eine Überprüfung der Umsetzung wird in der nächsten Berichtsperiode erfolgen.

4.2
Auskunfteien und Inkassounternehmen

4.2.1
DS-GVO:
Vorbereitung auf das Wirksamwerden der Datenschutz-Grundverordnung im Bereich der Auskunfteien

Durch umfangreiche Abstimmungen zwischen den Aufsichtsbehörden und mit den Auskunfteien wurde die Anwendung der DS-GVO ab dem 25.05.2018 vorbereitet.

Die Tätigkeit der Auskunfteien ist bisher datenschutzrechtlich durch nationales Recht, die §§ 28a, 28b und 29 BDSG, umfassend und detailliert reguliert. Diese Regelungen sind in der DS-GVO nicht mehr enthalten. Stattdessen richtet sich die Tätigkeit der Auskunfteien in Zukunft ganz wesentlich nach den sehr allgemeinen Vorschriften in Art. 6 DS-GVO.

Zwar können die bisherige Rechtslage und die in den §§ 28 ff. BDSG kodifizierten Grundsätze durch eine entsprechende Auslegung von Art. 6 Abs. 1f DS-GVO auch weiter zur Anwendung kommen. Mangels klarer Kodifizierung besteht jedoch ab Geltung der DS-GVO sowohl für die betroffenen Personen als auch für die Auskunfteien und Unternehmen, die deren Dienste nutzen, eine erhöhte Rechtsunsicherheit. Im Ergebnis könnte sich die Datenverarbeitung durch Auskunfteien erheblich ausweiten oder stark reduzieren, je nachdem, welche Auslegung der allgemeinen Regelungen des Art. 6 DS-GVO sich zukünftig etabliert.

Durch einen intensiven Abstimmungsprozess zwischen den Aufsichtsbehörden und mit den Auskunfteien konnte die Rechtsunsicherheit wie nachfolgend dargestellt abgemildert werden. Dazu wurden die wichtigsten Themen rechtlich geprüft und aufbereitet.

4.2.1.1
Zulässigkeit und Umfang von Bonitätsauskünften

Die Aufsichtsbehörden sind sich einig, dass die in den §§ 28 ff. BDSG kodifizierten Grundsätze im Rahmen der Anwendung von Art. 6 Abs. 1 b und f DS-GVO als Rechtsgrundlage für die Verarbeitung auch weiter zur Anwendung kommen können. Anfragen von verantwortlichen Stellen bei Auskunfteien zur Prüfung der Bonität im vorvertraglichen Bereich, aber auch Bonitätsabfragen etwa zur Prüfung der Erfolgsaussichten von Vollstreckungsmaßnahmen können grundsätzlich im Sinne von Art. 6 Abs. 1 b DS-GVO als erforderlich zur Durchführung vorvertraglicher oder vertraglicher Maßnahmen angesehen werden. Für die Erteilung einer Auskunft durch Auskunfteien bietet Art. 6 Abs. 1 f DS-GVO eine ausreichende Rechtsgrundlage. Dem stehen auch nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, entgegen. Es bleibt also bei der Interessenabwägung, die bisher gemäß §§ 28 Abs. 1 S. 1 Nr. 2 und 29 Abs. 2 BDSG durchgeführt werden musste und immer noch muss. Dies entspricht auch der Wertung von EG 47 DS-GVO. Wie bisher kann ein bestehendes oder drohendes kreditorisches Risiko die Rechtmäßigkeit einer Bonitätsabfrage indizieren.

Auf einen vorherigen Nachweis der Zulässigkeit einer Bonitätsabfrage gegenüber der Auskunftei kann verzichtet werden. Zwar enthält die DS-GVO nicht mehr die grundsätzliche Privilegierung der Bonitätsabfrage nach § 29 Abs. 2 BDSG. Die Forderung eines Einzelnachweises und dessen Speicherung bzw. Aufbewahrung ist im Massengeschäft jedoch überzogen. Sie würde berechtigte und zulässige Datenübermittlungen aus rein formalen Gründen vereiteln. Vielmehr wird es auch weiterhin ausreichen, wenn das berechtigte Interesse glaubhaft gemacht wird. Mangels ausdrücklicher gesetzlicher Privilegierung kann jedoch nicht mehr von einer generellen Zulässigkeit der bloßen Glaubhaftmachung ausgegangen werden. Dies gilt vielmehr nur dann, wenn aufgrund bisheriger Erfahrungen oder begründeter Erwartungen die Gewissheit besteht, dass Bonitätsabfragen nur dann durchgeführt werden, wenn diese zulässig sind. Das Maß der Gewissheit muss dabei Zweifeln an der Zulässigkeit Schweigen gebieten, ohne sie völlig auszuschließen.

Dies erfordert eine ausreichende Organisationsstruktur, welche unzulässige Bonitätsabfragen verhindert oder zumindest so weit erschwert, dass verbleibenden Zweifeln an dem Unterbleiben unzulässiger Bonitätsabfragen Schweigen geboten wird. Hierfür wird in der Regel die Protokollierung der Bonitätsabfragen inkl. der Person des Abfragenden durch individualisierte und personalisierte Zugangsberechtigungen erforderlich sein. Einzelne Fehlabfragen beeinträchtigen die Zulässigkeit nicht. Mehrfache unzulässige Abfragen oder eine vollständig fehlende Vorsorge gegen unzulässige Abfragen vermögen die grundsätzlich bestehende Vermutung, dass Bonitätsabfragen zulässig sind, aber zu entkräften. In solchen Fällen können Bonitätsauskünfte im Massengeschäft nicht mehr zulässig erteilt werden.

4.2.1.2
Zulässigkeit und Umfang der Datenspeicherung

Informationen über negative Erfahrungen mit dem Zahlungsverhalten einer betroffenen Person können ebenfalls gemäß Art. 6 Abs. 1 f DS-GVO an eine Auskunftei übermittelt und dort gespeichert werden. Auch hier ist eine Abwägung durchzuführen, die zugunsten der Übermittlung ausfällt, wenn die bisher in § 28a Abs. 1 BDSG kodifizierten Voraussetzungen vorliegen. Nur dann ist sicher gewährleistet, dass ein Sachverhalt vorliegt, der zuverlässig auf eine verminderte oder eingeschränkte Bonität einer betroffenen Person schließen lässt. Mangels ausdrücklicher Kodifizierung darf die Prüfung der Voraussetzungen des § 28a Abs. 1 BDSG jedoch nicht zu formell wörtlich, sondern nach Sinn und Zweck betrachtet werden. Sachverhalte, bei denen eindeutig kein bonitätsrelevanter Sachverhalt vorliegt, wie bspw. die Geltendmachung von behaupteten, aber in der Regel zweifelhaften Ansprüchen, rechtfertigen eine Übermittlung daher nicht. Dient die Übermittlung daher nur der Drohung oder Durchsetzung sehr zweifelhafter Ansprüche, wäre sie unzulässig.

Das berechtigte Interesse an der Übermittlung der Negativinformationen besteht zum einen in dem Interesse Dritter, über negative Zahlungserfahrungen informiert zu werden, um eigenen negativen Erfahrungen vorzubeugen; Art. 6 Abs. 1 b DS-GVO. Zum anderen besteht es in dem Interesse des übermittelnden Unternehmens, an einem solchen System teilnehmen zu können und ebenfalls über negative Erfahrungen Dritter informiert zu werden; Art. 6 Abs. 1 f DS-GVO.

Die Interessen der betroffenen Personen stehen dem nicht entgegen, wenn die Tatsache der negativen Zahlungserfahrung hinreichend sicher ist und dieses Verhalten nach empirischer Erfahrung oder statistischer Auswertung ebenfalls hinreichend sicher auf eine verminderte oder eingeschränkte Bonität einer betroffenen Person und die damit verbundene erhöhte Wahrscheinlichkeit eines Ausfalls schließen lässt. Zusätzlich ist zu berücksichtigen, dass durch die Übermittlung auch betroffene Personen vor dem Eingehen zu hoher Risiken oder einer zu hohen Verschuldung geschützt werden können.

4.2.1.3

Zulässigkeit und Umfang des Scorings

Die bisher in den §§ 6a und 28b BDSG geregelten Sachverhalte des Scorings und der automatisierten Einzelentscheidung sind in der DS-GVO in den Art. 22 (automatisierte Entscheidung) und 4 Ziff. 4 (Profiling) enthalten. Die bisher vorhandenen inhaltlichen Vorgaben für das Scoring sind in der DS-GVO jedoch nicht mehr enthalten. Stattdessen enthält EG 71 DS-GVO einige Hinweise auf die Erfordernisse bei der automatisierten Entscheidungsfindung.

Profiling wird in Art. 4 Nr. 4 DS-GVO definiert als jede Art der Analyse personenbezogener Daten zur Vorhersage eines künftigen Ereignisses. Inhaltliche Beschränkungen enthält die DS-GVO nicht. Andererseits enthält Art. 4 Nr. 4 DS-GVO auch keine Rechtsgrundlage für die Durchführung des Profilings. Eine solche ist in jedem Fall des Profilings erforderlich. Sie muss nicht nur die Speicherung und Verarbeitung der Daten, sondern auch das Profiling explizit umfassen.

Grundsätzlich kommt für das Profiling vor allem Art. 6 Abs. 1 b und f DS-GVO als Rechtsgrundlage in Betracht. Profiling wird im Regelfall nach der gleichen Rechtsgrundlage zu beurteilen sein wie die Verarbeitung der dem Profiling zugrundliegenden Daten. Für Auskunfteien ist dies vor allem Art. 6 Abs. 1 f DS-GVO.

Verträge von Unternehmen, die grundsätzlich ein kreditorisches Risiko beinhalten, rechtfertigen die Durchführung eines Profilings sowohl im vorvertraglichen Stadium als auch während ihrer Durchführung nach der Rechtsgrundlage für die Verarbeitung der Daten. Die gesonderte Begründung ergibt sich aus dem möglichen Vertragsrisiko. Die Zulässigkeit schließt den Bezug von Profilingwerten von Auskunfteien ein. Ob ein periodischer Bezug von Profilingwerten gerechtfertigt ist, bedarf indes einer eigenen Prüfung.

Profiling ist nach Art. 6 Abs. 1 DS-GVO nur rechtmäßig, wenn zur Berechnung des Wahrscheinlichkeitswertes „geeignete mathematische oder statistische Verfahren" eingesetzt werden, EG 71 DS-GVO. Die derzeit üblichen Verfahren der Regressionsanalyse dürften diesen Anforderungen gerecht werden, sofern und soweit nur risikorelevante Merkmale eingesetzt werden. Im Zweifel ist die Risikorelevanz eines Merkmals statistisch nachzuweisen.

Zusätzlich sind die Anforderungen von Art. 22 DS-GVO zu berücksichtigen, wenn das Ergebnis eines Profilings automatisiert weiterverarbeitet wird. Für Unternehmen kommt dabei die Zulässigkeit der Entscheidungsfindung nach Art. 22 Abs. 2 DS-GVO in Betracht. In der Regel wird die Vorbereitung einer Entscheidung oder das Treffen der Entscheidung im Rahmen des Risikomanagements eines Unternehmens erforderlich sein. Dies ist jedenfalls dann der Fall, wenn die Entscheidung im Massenverfahren oder schnell getroffen werden muss.

Ergänzend sind jedoch Maßnahmen zu treffen, welche auf Wunsch der betroffenen Person eine nicht automatisierte Nachentscheidung gemäß Art. 22 Abs. 3 DS-GVO ermöglichen. Die Struktur der Vorschrift entspricht jedoch dem bisherigen § 6a BDSG, so dass die vorhandenen Geschäftsprozesse die Anforderungen im Grundsatz erfüllen dürften. Um den betroffenen Personen die Ausübung des in Art. 22 Abs. 3 DS-GVO enthaltenen Rechts zu ermöglichen, das nicht nur bei einer ablehnenden Entscheidung besteht, ist im Gegensatz zur bisherigen Rechtslage die Durchführung einer automatisierten Entscheidungsfindung auch bei einer genehmigenden Entscheidung transparent zu machen. Die besonderen Anforderungen an die Verarbeitung von besonderen Kategorien personenbezogener Daten gemäß Art. 22 Abs. 4 DS-GVO sind ebenfalls zu beachten.

Eine Verarbeitung von Daten aus sozialen Netzwerken oder ähnlichen Quellen ist ebenfalls an Art. 6 DS-GVO zu messen. Alleine aus der möglicherweise freien Zugänglichkeit dieser Daten ergibt sich eine Rechtmäßigkeit ihrer Verwendung im Profiling nicht. Daten werden in sozialen Netzwerken nicht mit dem Zweck eingegeben, diese im Rahmen von Profilings zu nutzen. Mit einer derartigen Verwendung muss ein Nutzer sozialer Netzwerke auch nicht rechnen, was nach EG 47 und 50 DS-GVO Voraussetzung für deren Verarbeitung wäre. Art. 6 Abs. 1 b bis f DS-GVO scheidet folglich als Rechtsgrundlage aus. In Betracht kommt allenfalls eine Nutzung dieser Daten im Rahmen einer Einwilligung gemäß Art. 6 Abs. 1 a DS-GVO. Die erhöhten Anforderungen an die Freiwilligkeit nach der DS-GVO sind dabei zu beachten. Eine Ablehnung der Vertragsbeziehung wegen einer nicht erteilten Einwilligung in das Profiling scheidet daher gemäß Art. 7 Abs. 4 DS-GVO aus.

4.2.1.4
Speicherfristen

Speicherfristen für Auskunfteien sind derzeit in § 35 Abs. 2 Satz 2 Nr. 4 BDSG detailliert geregelt. Eine derart detaillierte Regelung enthält die DS-GVO nicht mehr. Art. 17 DS-GVO gibt betroffenen Personen zwar einen Anspruch auf Löschung gespeicherter personenbezogener Daten. Detaillierte Prüf- und Löschfristen sind aber nicht mehr enthalten. Stattdessen normiert die DS-GVO, dass Daten zu löschen sind, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind; Art. 17 Abs. 1 a DS-GVO. Wann dies exakt der Fall ist, lässt die DS-GVO jedoch offen.

Zur Schaffung von Rechtssicherheit haben die Aufsichtsbehörden mit den Auskunfteien eine Beibehaltung der bisherigen Fristen besprochen. Zur Gleichbehandlung der betroffenen Personen könnten die Fristen allerdings künftig einheitlich ab der Speicherung und nicht – wie bisher – ab dem Ende des Jahres der Speicherung berechnet. Dies wird die Fristen voraussichtlich etwas verkürzen.

Es ist beabsichtigt, dieses Ergebnis im Wege der Selbstverpflichtung umzusetzen.

4.2.1.5
Umfang von Selbstauskünften

Der Umfang von Selbstauskünften ergibt sich künftig vor allem aus Art. 15 DS-GVO. Auch hier enthält die DS-GVO nicht mehr die detaillierten Regelungen für Auskunfteien gemäß § 34 BDSG.

Betroffenen Personen ist jedoch gemäß Art. 15 Abs. 3 DS-GVO eine vollständige Kopie der gespeicherten Daten zur Verfügung zu stellen. Dies umfasst die bisher erteilten Auskünfte jedenfalls dann, wenn diese gespeichert sind.

Durch die umfangreichen Abstimmungsverfahren und die damit verbundene Erzielung von Ergebnissen besteht im Tätigkeitsbereich der Auskunfteien ab der Geltung des DS-GVO eine deutlich verbesserte Rechtssicherheit für betroffene Personen und die Wirtschaft.

4.2.2
SCHUFA Holding AG

Aufgrund ihrer hervorgehobenen Stellung im Bereich der Handelsauskunfteien bildet die Kontrolle der SCHUFA Holding AG (SCHUFA) einen Schwerpunkt meiner Tätigkeit. Die erheblichen Beeinträchtigungen, die Betroffene durch die Speicherung von Vorfällen erleiden, die sich negativ auf die Bonität auswirken, führen zu einer großen Anzahl von Beschwerden. Verstöße gegen datenschutzrechtliche Vorschriften durch die SCHUFA sind jedoch angesichts des Umfangs an verarbeiteten Daten selten.

4.2.2.1
Auskunftserteilung gemäß § 34 BDSG

Auch in diesem Berichtszeitraum erhielt ich Beschwerden sowie Anfragen zur Auskunftserteilung der SCHUFA. Diese betrafen sowohl die Voraussetzungen der Auskunftserteilung (Möglichkeiten der Identifizierung der betroffenen Person) als auch die Modalitäten der Übermittlung der Auskunft an die betroffene Person, wie etwa die Zustellung der Datenübersicht an einen anderen Ort als die Meldeanschrift des Betroffenen.

Die SCHUFA ist gemäß § 34 BDSG verpflichtet, der betroffenen Person auf deren Begehren Auskunft über die dort zu ihrer Person gespeicherten Daten zu erteilen. Hierzu hat sie als verantwortliche Stelle zu gewährleisten, Auskünfte ausschließlich an die betroffenen Personen zu erteilen. Schließlich ist die unbefugte Übermittlung personenbezogener Daten einer betroffenen Person an Dritte unzulässig.

4.2.2.1.1

Identifikation der betroffenen Person

Zur Gewährleistung einer ordnungsgemäßen Beauskunftung der betroffenen Person hat die SCHUFA diese zunächst zweifelsfrei zu identifizieren.

Grundsätzlich ist es nicht erforderlich, dem Auskunftsersuchen eine Kopie des Personalausweises beizufügen. Sofern der SCHUFA jedoch eine eindeutige und zweifelsfreie Identifizierung des Auskunftsersuchenden/der betroffenen Person anhand der von diesem/-r übermittelten Daten nicht möglich ist (beispielsweise bei abweichenden Adressdaten), fordert die SCHUFA Holding AG den Auskunftsersuchenden auf, eine Fotokopie des Ausweisdokuments bzw. der Einwohnermeldeamtsbestätigung zu übermitteln.

Zur Frage der etwaigen Zulässigkeit der Anforderung von Personalausweiskopien nehme ich Bezug auf meine Erläuterungen im Rahmen meines 41. Tätigkeitsberichts (Ziff. 2.1.2) sowie im Rahmen meines 42. Tätigkeitsberichts (Ziff. 4.3.4).

Eine betroffene Person richtete die Frage an mich, inwieweit die SCHUFA berechtigt sei, die Vorlage einer Einwohnermeldeamtsbestätigung von ihr zu begehren, sofern diese sich gegenüber der SCHUFA mit einem ausländischen Pass, dem keine Anschriftendaten zu entnehmen seien, ausweisen könne.

Bei derart gelagerten Sachverhalten ist die Vorlage der Meldebescheinigung (die jeder Bürger im Rahmen der Um- oder Anmeldung seines Wohnsitzes seitens des Einwohnermeldeamts ausgehändigt bekommt) gegenüber der SCHUFA erforderlich. Dabei können auf der Kopie dieser Bescheinigung Schwärzungen der Daten durch die betroffene Person vorgenommen werden, wenn diese Daten zur Identifikation nicht erforderlich sind, wie etwa die Religionszugehörigkeit.

Durch die Vorlage der Meldebescheinigung wird die SCHUFA in die Lage versetzt, die aktuelle Wohnanschrift der betroffenen Person, an die die Auskunft gesandt werden wird, zu verifizieren und die betroffene Person zu identifizieren. Gegebenenfalls kann es zur eindeutigen Zuordnung des SCHUFA-Datensatzes zu den im Rahmen des Auskunftsersuchens angegebenen Daten der betroffenen Person erforderlich sein, deren Voranschrift nachzuweisen. Auch hierfür ist die Meldebescheinigung geeignet.

Das vorausgeführte Verfahren dient der zweifelsfreien Identifizierung des Auskunftsersuchenden bzw. der zweifelsfreien Zuordnung eines SCHUFA-Datensatzes zu der betroffenen Person und wird meinerseits nicht bemängelt.

4.2.2.1.2

Versand der Auskunft an eine innerdeutsche Postfachadresse

Vereinzelt beschwerten sich betroffene Personen darüber, dass die SCHUFA sich weigere, die Auskunft an eine innerdeutsche Postfachadresse zu senden.

Diese Weigerung der SCHUFA ist aus datenschutzrechtlicher Sicht jedoch geboten. Nach Mitteilung der Deutsche Post AG erfolgt bei dem Vertragsschluss zur Einrichtung eines Postfachs eine Identifizierung der betroffenen Personen – anders als beim PostIdent-Verfahren – nicht. Darüber hinaus ist eine Postfachadresse weder auf dem Personalausweis noch auf einem Reisepass oder einer amtlichen Meldebescheinigung vermerkt. Mithin ist es der SCHUFA als verantwortlicher Stelle nicht möglich, die seitens des Auskunftsersuchenden angegebene Postfachadresse als diejenige der betroffenen Person zweifelsfrei zu verifizieren. Somit bestünde die Gefahr einer unzulässigen Datenübermittlung an einen unberechtigten Dritten durch die SCHUFA. Eine derartige Auskunftspraxis würde ich der SCHUFA folglich untersagen.

4.2.2.1.3

Erteilung einer Selbstauskunft an ein Obdachlosenheim

Eine betroffene Person wohnte nach der Rückkehr von einem längeren Auslandsaufenthalt in einem Obdachlosenwohnheim und war dort auch gemeldet. Die Adresse des Obdachlosenwohnheims war als aktuelle Anschrift in ihrem Personalausweis angegeben. Unter Beifügung einer Kopie dieses Ausweises beantragte die betroffene Person eine

Selbstauskunft nach § 34 BDSG und bat darum, diese an sie, wohnhaft in dem Obdachlosenheim, zu senden. Die SCHUFA lehnte den Versand an das Obdachlosenheim ab. An Anschriften, die den Zusatz „wohnhaft bei“ trügen, könne generell keine Selbstauskunft versandt werden.

Diese Auffassung ist grundsätzlich nicht zu bemängeln. Wird die Zusendung einer Selbstauskunft beantragt, ist sicherzustellen, dass die Selbstauskunft die betroffene Person erreicht. Die Versendung an Dritte zur Weiterleitung an die betroffene Person darf grundsätzlich nicht erfolgen, weil dies das Risiko beinhaltet, dass die Selbstauskunft einem Dritten preisgegeben wird. Zu berücksichtigen ist dabei auch, dass bei der schriftlichen Beantragung einer Selbstauskunft die antragstellende Person nicht sicher authentifiziert werden kann. Ein schriftlicher Antrag kann von einer anderen Person leicht gefälscht werden. Bei einer Versendung an eine andere Anschrift als die aktuelle Wohnanschrift wäre es deshalb prinzipiell möglich, die Selbstauskunft für eine andere Person zu beantragen und auch zu erhalten. Die betroffene Person würde dies in der Regel nicht bemerken. Wird die beantragte Selbstauskunft jedoch ausschließlich an eine verifizierte Adresse der betroffenen Person versendet, ist das Risiko einer Kenntnisnahme durch einen Dritten minimiert.

Der Versand einer Selbstauskunft an eine nicht verifizierte Adresse mit dem Zusatz „wohnhaft bei“ ist datenschutzrechtlich zu beurteilen wie der Versand an einen Dritten zur Weiterleitung an die betroffene Person. Ein derartiger Versand würde den Missbrauch der Selbstauskunft begünstigen. Daher kann – worauf die SCHUFA zu Recht hingewiesen hat – eine Versendung an eine andere Anschrift als die aktuelle Wohnanschrift unter Beifügung eines Zusatzes nicht erfolgen.

Bei der vorliegenden Beschwerde war die betroffene Person jedoch in dem Obdachlosenwohnheim gemeldet und die Anschrift des Obdachlosenwohnheims war auch im Personalausweis eingetragen. Die Anschrift war damit ausreichend verifiziert. Zusätzlich gab es für die betroffene Person keine andere Möglichkeit, die Selbstauskunft zu erhalten. Die oben dargelegten Grundsätze waren daher ausnahmsweise nicht anwendbar. Dies hatte die SCHUFA in der Massenbearbeitung von Anträgen auf Selbstauskunft offenbar übersehen.

Nachdem ich die SCHUFA auf diesen Umstand hingewiesen hatte, wurde die Selbstauskunft unverzüglich erteilt.

4.2.2.1.4

Versand der Auskunft an eine private c/o-Anschrift

Einzelne betroffene Personen beschwerten sich außerdem über die Weigerung der SCHUFA, die Auskunft an eine private c/o-Anschrift zu senden.

Diese Weigerungen der SCHUFA wurden meinerseits ebenfalls nicht beanstandet. Schließlich ist es der SCHUFA auch bei diesem Sachverhalt nicht möglich auszuschließen, dass ein unbefugter Dritter in Besitz der SCHUFA-Datenübersicht gelangt und damit Kenntnis von den Daten der betroffenen Person erhält.

4.2.2.1.5

Versand der Auskunft an ein bevollmächtigtes Organ der Rechtspflege

In einem weiteren Fall beschwerte sich eine betroffene Person über die Weigerungen der SCHUFA, die Auskunft an ein bevollmächtigtes Organ der Rechtspflege (beispielsweise Rechtsanwalt oder Notar) zu senden. Im Rahmen seines Auskunftsersuchens gab der Betroffene jedoch seine Wohnanschrift nicht an, sondern begehrte die Zustellung der Auskunft an ein von ihm bezeichnetes staatliches Notariat in Baden-Württemberg.

Grundsätzlich ist der Versand der Datenübersicht an diese Organe möglich. Hierbei ist jedoch die erteilte Vollmacht jeweils einer individuellen Prüfung zu unterziehen. Aus dieser muss die Bevollmächtigung des konkret bezeichneten Organs zur Empfangnahme der Auskunft zweifelsfrei hervorgehen.

Da bei Anwaltskanzleien oder Notariaten in der Regel eingehende Post routinemäßig durch deren Mitarbeiter geöffnet wird, was zu deren Kenntnisnahme der Daten der betroffenen Person führen kann, sollte sich das Einverständnis der betroffenen Person mit diesem Sachverhalt ebenfalls der Vollmacht entnehmen lassen.

Ferner muss auch dieses Organ seitens der betroffenen Person durch Vorlage geeigneter Unterlagen (Personalausweis, Pass, Meldebescheinigung) in die Lage versetzt werden, den Betroffenen vor Aushändigung der Datenübersicht zweifelsfrei zu identifizieren.

Im vorliegenden Fall ergab meine Prüfung des Sachverhalts jedoch, dass der SCHUFA bereits anhand der Angaben der betroffenen Person eine zweifelsfreie Identifizierung der betroffenen Person bzw. Zuordnung zu einem SCHUFA-Datensatz tatsächlich nicht möglich war. Bereits aus diesem Grunde begrüßte ich die Weigerung der SCHUFA, im konkreten Fall keine Auskunft zu erteilen, ausdrücklich.

4.2.2.1.6
Zeitpunkt der Auskunftserteilung

Mehrere betroffene Personen erkundigten sich bei mir, innerhalb welcher Frist die SCHUFA die Auskunft nach § 34 BDSG zu erteilen habe. Eine betroffene Person fragte mich, ob eine Fristsetzung zur Auskunftserteilung gegenüber der SCHUFA sinnvoll sei. Darüber hinaus beschwerten sich betroffene Personen wiederholt darüber, dass die SCHUFA die Auskunft verspätet oder nicht innerhalb ihrer gesetzten Frist erteilt habe.

Der Gesetzgeber hat eine konkrete Frist, innerhalb derer eine Auskunftei eine Auskunft zu erteilen hat, im BDSG nicht normiert. Grundsätzlich kann zwar aus einer nicht im BDSG normierten Frist abgeleitet werden, dass die Auskunftserteilung unverzüglich nach Eingang des Auskunftsersuchens bei der verantwortlichen Stelle zu erfolgen hat. Dies insbesondere im Hinblick auf § 43 Abs. 1 Nr. 8a BDSG, wonach ordnungswidrig handelt, wer entgegen § 34 Abs. 1 Satz 1 BDSG eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt. Unverzüglich in diesem Sinne bedeutet jedoch nicht sofort, sondern vielmehr ist die Auskunft ohne schuldhaftes Zögern zu erteilen. Hierbei sind jedoch auch die betrieblichen Erfordernisse der verantwortlichen Stelle zu berücksichtigen und dieser ist eine angemessene Bearbeitungsdauer zur Erstellung der Auskunft einzuräumen.

Gerade vor dem Hintergrund des Umfangs und der Komplexität der Auskunft der SCHUFA nach § 34 BDSG (insbesondere die Errechnung und Darstellung diverser unterschiedlicher Branchen-Wahrscheinlichkeitswerte) wird eine Auskunftserteilung durch diese innerhalb eines Zeitraumes von durchschnittlich drei Wochen meinerseits nicht beanstandet.

Vor dem Hintergrund dieser Betrachtung sind Fristsetzungen durch betroffene Personen in diesem Zusammenhang nicht erforderlich. Unabhängig davon waren die vorliegenden Fristsetzungen der betroffenen Personen von ein bis zwei Wochen ab Erstellungsdatum des jeweiligen Auskunftsersuchens deutlich zu knapp bemessen.

In vereinzelten Fällen sah ich mich veranlasst, die SCHUFA auf eine zügigere Beauskunftung hinzuweisen. Eine Einhaltung der vorausgeführten durchschnittlichen Bearbeitungsdauer der Auskunftserteilung konnte erreicht werden.

4.2.2.2
Sperrung eines Eintrags nach dem Bestreiten von dessen Richtigkeit

In einer weiteren Beschwerde bestand zwischen der SCHUFA und einer betroffenen Person Streit über die Richtigkeit und Berechtigung eines einzelnen Merkmals. Die Titulierung der dem Merkmal zugrundeliegenden Forderung und das fehlende Bestreiten der Forderung wurden vom Vertragspartner der SCHUFA bestätigt. Das Merkmal basierte auf einer zum Zeitpunkt der Einreichung der Beschwerde bereits erledigten Forderung.

Unter Zugrundelegung dieses Sachverhaltes war die SCHUFA berechtigt, das Merkmal zu speichern. Die Berechtigung zur Speicherung ergab sich aus § 28a Abs. 1 Nr. 1 BDSG. Danach dürfen titulierte Forderungen gespeichert werden, wenn diese nicht unverzüglich beglichen werden. Ein unverzügliches Begleichen wurde mir gegenüber durch die betroffene Person nicht vorgetragen. Mit Erledigung der Forderung war die Speicherung auch nicht sofort aufzuheben. Vielmehr darf die Forderung in den Fristen von § 35 Abs. 2 Nr. 4 BDSG weiter gespeichert werden.

Dennoch befanden sich die Parteien in einem Rechtsstreit über die Berechtigung der SCHUFA zur Speicherung des Merkmals. Lässt sich weder die Richtigkeit noch die Unrichtigkeit der gespeicherten Daten feststellen, sind diese grundsätzlich nach § 35 Abs. 4 BDSG zu sperren. Dabei darf die Tatsache der Sperrung nicht übermittelt werden, § 35 Abs. 4a BDSG. Aufgrund des Rechtsstreits wurde von der SCHUFA nicht nur der bestrittene Eintrag, sondern der gesamte Datensatz gesperrt. Dadurch wurde über die betroffene Person auf Bonitätsanfragen von Vertragspartnern der SCHUFA keine Auskunft mehr erteilt. Dies führte ähnlich einer negativen Bonitätsauskunft dazu, dass der betroffenen Person keine Kredite gewährt wurden.

Die Erteilung von Auskünften durch Wirtschaftsauskunfteien lässt sich nicht ohne weiteres erzwingen. Zwar kann auch die fehlende Erteilung einer Auskunft eine falsche Auskunft darstellen, weil der betreffenden Handelsauskunftei die Person nebst unbestrittenen Merkmalen bekannt ist. Die Handelsauskunftei beruft sich jedoch in der Regel darauf, dass die erteilte Bonitätsauskunft ohne das bestrittene Merkmal eine falsche Bonität ausweist und eine ohne das Merkmal erteilte Auskunft damit ebenfalls falsch ist. Allerdings spricht die gesetzliche Wertung des § 35 Abs. 4 und 4a BDSG gegen diese Auffassung. Das Merkmal und die fehlende Möglichkeit der Handelsauskunftei, die Richtigkeit des gespeicherten Merkmals nachzuweisen, sollen sich nicht negativ auf die betroffene Person auswirken.

Im weiteren Verlauf der Beschwerdebearbeitung vertrat die SCHUFA jedoch die Auffassung, das bestrittene Merkmal sei richtig, und entschloss sich dazu, zu der betroffenen Person inkl. des bestrittenen Merkmals wieder Auskünfte zu erteilen. Dem Merkmal wurde richtigerweise der Zusatz beigefügt, dass der Eintrag bestritten sei.

Auf diese Vorgehensweise war § 35 Abs. 4 und 4a BDSG nicht anwendbar. Die SCHUFA war der Auffassung, die Richtigkeit des Merkmals ausreichend aufgeklärt zu haben, und konnte dies aufgrund der Stellungnahme des Vertragspartners, der das Merkmal gemeldet hatte, auch nachweisen. Der weiter bestehende Streit ist dafür ohne Belang. Zwar trägt die SCHUFA in diesem Fall das Risiko, dass sich die erteilte Auskunft später als falsch erweist und könnte dementsprechend schadensersatzpflichtig sein. Die SCHUFA war jedoch angesichts der bereits betriebenen Aufklärung um das Merkmal hinreichend sicher, dass eine Berechtigung zur Speicherung bestand. Dies konnte von mir nicht bemängelt werden.

4.2.2.3

Auffinden des Bestellformulars für eine Auskunftserteilung gemäß § 34 BDSG auf der Homepage der SCHUFA Holding AG

Immer wieder beschweren sich Betroffene über die Gestaltung der Homepage der SCHUFA. Gerügt wird dabei das Auffinden des Bestellformulars für eine kostenlose Auskunftserteilung nach § 34 BDSG. Die SCHUFA erschwere eine Beauskunftung der Betroffenen erheblich, indem diese ihre kostenpflichtigen Produkte derart in den Vordergrund stelle, dass das Bestellformular für eine kostenfreie Auskunft nach § 34 BDSG sehr schwer bis gar nicht zu finden sei. Darüber hinaus sei es aus technischen Gründen regelmäßig nicht möglich, das Bestellformular zu öffnen oder von der Homepage herunterzuladen.

Zutreffend ist, dass die SCHUFA auf ihrer Homepage ein Bestellformular für die Bestellung einer kostenfreien Auskunft nach § 34 BDSG sowie ein Erläuterungsblatt hierzu als PDF-Dokument zum Download bereitstellt.

Allerdings ist es grundsätzlich nicht erforderlich, zur Bestellung einer Auskunft nach § 34 BDSG ein bestimmtes Formular zu nutzen. § 34 BDSG sieht ein Formerfordernis nicht vor. Jeder Betroffene hat die Möglichkeit, mittels eines formlosen Schreibens eine Datenübersicht nach § 34 BDSG bei der SCHUFA zu bestellen.

Darüber hinaus verhindert die Gestaltung der Homepage der SCHUFA eine Auskunftserteilung nach § 34 BDSG nicht: Die Menüführung führt ohne erkennbare Hindernisse unmittelbar zu dem entsprechenden Bestellformular, welches sich in der Regel problemlos öffnen und speichern lässt. Sofern dieses Formular in Einzelfällen nicht geöffnet werden konnte, war in der Regel eine das Öffnen verhindernde Einstellung des Browsers die Ursache.

Mangels einer Verpflichtung der SCHUFA, überhaupt ein Formular bereitzustellen, und angesichts der auch ohne Verwendung des Formulars bestehenden Auskunftsverpflichtung konnte ich bisher keinen Verstoß gegen datenschutzrechtliche Bestimmungen erkennen.

4.2.3

Die Selbstauskunft gemäß § 34 BDSG ist in der Regel umfassend zu erteilen

Wird im Antrag auf Selbstauskunft nach § 34 BDSG nicht konkretisiert, auf welchen Bereich der Antrag beschränkt wird, ist die Selbstauskunft umfassend über alle Geschäftsbereiche eines Unternehmens zu erteilen.

Aufgrund einer Beschwerde wurde ich auf die Praxis einer Auskunftei bei der Bearbeitung von Selbstauskünften aufmerksam, die zu bemängeln war. Die Auskunftei war bisher nahezu ausschließlich im Bereich der Adressermittlung tätig. Durch die Zusammenarbeit mit einer auf Bonitätsauskünfte spezialisierten Auskunftei wurde das Geschäftsfeld auf Bonitätsauskünfte ausgeweitet. Dem Beschwerdeführer wurde auf seinen Antrag auf Selbstauskunft eine an sich nicht zu bemängelnde, aber auf den Geschäftsbereich der Adressermittlung beschränkte Auskunft erteilt.

Mit Auskunfteien, die Bonitätsinformationen lediglich über den Zugang zu einem Kooperationspartner als Reseller vermitteln, hatte ich mich bereits im 44. Tätigkeitsbericht (Ziff. 4.3.4) befasst. Auf Durchleite- oder Resellerauskunfteien sind die Regelungen des BDSG zu Auskunfteien in vollem Umfang anzuwenden. Daraus folgt, dass diese im Rahmen von Selbstauskünften über erteilte Auskünfte in vollem Umfang auskunftspflichtig sind.

Die Auskunftei wurde von mir auf diese Rechtslage hingewiesen und hat zugesichert, dies zukünftig zu beachten. Zwangsmaßnahmen waren nicht erforderlich.

4.2.4

Versendung von Fragebogen an Arbeitgeber vor einer Pfändung von Arbeitseinkommen

Der Versendung von Fragebogen zur Pfändbarkeit von Arbeitseinkommen an Arbeitgeber durch Inkassounternehmen ist zulässig, wenn die Fragen auf das unbedingt erforderliche Mindestmaß beschränkt werden.

Aufgrund einer Beschwerde wurde ich auf die Praxis eines großen Inkassounternehmens zur Vorprüfung der Pfändbarkeit von Arbeitseinkommen aufmerksam. Das Inkassounternehmen versendete Fragebogen an Arbeitgeber, in denen um Auskunft zum Arbeitseinkommen eines Arbeitnehmers gefragt wurde. Hierzu sollte durch den Arbeitgeber ein vorbereitetes Formular ausgefüllt werden, in welches detaillierte Angaben zum Arbeitseinkommen, der Steuerklasse, dem Familienstatus, zu Vorpfändungen, zum Bezug von Krankengeld und der Krankenkasse eingetragen werden konnten. Zwar war weder in dem Fragebogen noch in dem Anschreiben an den Arbeitgeber auf eine Verpflichtung zum Ausfüllen des Fragebogens hingewiesen worden. Ein ausdrücklicher Hinweis auf die Freiwilligkeit der Beantwortung fehlte jedoch.

Das Inkassounternehmen wies auf mein Befragen darauf hin, dass eine Beantwortung durch den Arbeitgeber Kosten für erfolglose Vollstreckungsmaßnahmen sparen könne. Diese Kosten seien letztlich durch den Schuldner und Arbeitnehmer zu tragen, weshalb die Beantwortung in dessen Interesse sei.

Eine derartige detaillierte Abfrage ist unzulässig, weil es dafür keine Rechtsgrundlage gibt.

Ein Arbeitgeber ist grds. nicht verpflichtet, derartige Anfragen zu beantworten. Erst nach einer Pfändung besteht gemäß § 840 ZPO eine Verpflichtung des Arbeitgebers als Drittschuldner der gepfändeten Forderung, sich zu der gepfändeten Forderung zu erklären.

§ 840 ZPO

(1) Auf Verlangen des Gläubigers hat der Drittschuldner binnen zwei Wochen, von der Zustellung des Pfändungsbeschlusses an gerechnet, dem Gläubiger zu erklären:

1. ob und inwieweit er die Forderung als begründet anerkenne und Zahlung zu leisten bereit sei;
2. ob und welche Ansprüche andere Personen an die Forderung machen;
3. ob und wegen welcher Ansprüche die Forderung bereits für andere Gläubiger gepfändet sei;
4. ob innerhalb der letzten zwölf Monate im Hinblick auf das Konto, dessen Guthaben gepfändet worden ist, nach § 850l die Unpfändbarkeit des Guthabens angeordnet worden ist, und
5. ob es sich bei dem Konto, dessen Guthaben gepfändet worden ist, um ein Pfändungsschutzkonto im Sinne von § 850k Abs. 7 handelt.

(2) Die Aufforderung zur Abgabe dieser Erklärungen muss in die Zustellungsurkunde aufgenommen werden. Der Drittschuldner haftet dem Gläubiger für den aus der Nichterfüllung seiner Verpflichtung entstehenden Schaden.

(3) Die Erklärungen des Drittschuldners können bei Zustellung des Pfändungsbeschlusses oder innerhalb der im ersten Absatz bestimmten Frist an den Gerichtsvollzieher erfolgen. Im ersteren Fall sind sie in die Zustellungsurkunde aufzunehmen und von dem Drittschuldner zu unterschreiben.

Darüber hinaus ergibt sich aus dem Anstellungsverhältnis in Verbindung mit § 32 BDSG die grundsätzliche Verpflichtung des Arbeitgebers zur vertraulichen Behandlung des Inhalts der Personalakte. Dies umfasst auch das Arbeitseinkommen des Arbeitnehmers.

Allerdings hat auch der Arbeitgeber ein Interesse an der Funktionsfähigkeit seiner Arbeitsprozesse. Durch die Pfändung von Arbeitseinkommen können die Betriebsabläufe beeinträchtigt werden und der Arbeitgeber kann einem finanziellen Risiko aus der fehlerhaften Behandlung von Pfändungen ausgesetzt sein. Für kleine bis mittelgroße Unternehmen kann die Pfändung von Arbeitseinkommen die Hilfe von Dritten, z. B. von Rechtsanwälten oder Steuerberatern, erfordern. Dadurch können weitere Kosten entstehen.

Das Inkassounternehmen, welches eine titulierte Forderung verfolgt, hat ein anerkennenswertes Interesse an der Klärung der Einkommensverhältnisse und des Bestehens eines Anstellungsverhältnisses vor Erlass eines Pfändungs- und Überweisungsbeschlusses. Durch eine sachgerechte Aufklärung der

Pfändungsmöglichkeiten bei einem Arbeitgeber kann durchaus interessengerecht für alle Beteiligten das Entstehen unnötiger Kosten sowie unnötiger Arbeitsaufwand vermieden werden.

Vollstreckungsversuche durch den Gläubiger oder das von ihm beauftragte Inkassounternehmen können sich auch für den Arbeitnehmer nachteilig auswirken. Insbesondere bei kleineren Unternehmen kann eine Pfändung sogar den Verlust des Arbeitsplatzes bedeuten, wenn aufgrund der Größe des Unternehmens das Kündigungsschutzgesetz keine Anwendung findet und der Arbeitgeber die Risiken und Kosten einer Pfändung scheut. Die Kosten von Vollstreckungsmaßnahmen sind zudem grundsätzlich durch den Schuldner/Arbeitnehmer zu tragen, § 788 Abs. 1 Satz 1 ZPO.

> § 788 Abs. 1 ZPO
>
> Die Kosten der Zwangsvollstreckung fallen, soweit sie notwendig waren (§ 91), dem Schuldner zur Last; sie sind zugleich mit dem zur Zwangsvollstreckung stehenden Anspruch beizutreiben.
> …

Daher kommt eine Beantwortung von Fragen zur Pfändbarkeit von Arbeitseinkommen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht. Wenn die Pfändung von Arbeitseinkommen beabsichtigt ist und unmittelbar bevorsteht, besteht ein berechtigtes Interesse des Arbeitgebers an der Beantwortung von Fragen zur Pfändbarkeit des Arbeitseinkommens. Die Fragen an den Arbeitgeber dürfen jedoch keinen Ausforschungscharakter haben und lediglich die Entscheidung über die Beantragung eines Pfändungs- und Überweisungsbeschlusses vorbereiten. Daher hat sich die Beantwortung auf die erforderlichen Informationen zu beschränken. Erforderlich ist lediglich die Angabe des pfändbaren Anteils am Arbeitseinkommen. Weitere Fragen sind auch unter der Annahme unzulässig, dass Arbeitgeber die Berechnung des pfändbaren Anteils häufig nicht sicher ermitteln können. Dieses Problem kann dadurch gelöst werden, dass dem Arbeitgeber ein Berechnungsschema zur Verfügung gestellt wird.

Zusätzlich muss vorher der Versuch unternommen worden sein, die benötigten Informationen direkt beim Arbeitnehmer zu erheben. Liegen dann noch die Voraussetzungen für den Erlass eines Pfändungs- und Überweisungsbeschlusses vor, überwiegen die Interessen des Arbeitnehmers nicht mehr. Die angefragten Informationen wären bei einer Pfändung nach § 840 ZPO ohnehin zu übermitteln. Die Informationen zum Vorliegen eines pfändbaren Anteils am Arbeitseinkommen dürfen daher zur Vermeidung weiteren Aufwands und weiterer Kosten übermittelt werden.

Dem Arbeitgeber ist das Vorliegen der vorstehend beschriebenen Voraussetzungen zu versichern. Nur wenn der Arbeitgeber in die Lage versetzt wird, die Zulässigkeit der Übermittlung zu überprüfen, kann er die Anfrage rechtssicher beantworten.

Mangels gesetzlicher Verpflichtung zur Beantwortung von Fragen zur Pfändbarkeit von Arbeitseinkommen kann die Beantwortung solcher Fragen nur freiwillig erfolgen. Hierauf ist der Arbeitgeber hinzuweisen.

Soweit die Übermittlung von Informationen unzulässig wäre, darf danach durch ein Inkassounternehmen auch nicht gefragt werden. Dies wurde von dem betroffenen Inkassounternehmen akzeptiert und sowohl das Formular als auch der gesamte Geschäftsprozess wurden freiwillig datenschutzkonform angepasst.

4.2.5
Auskunftserteilung gemäß § 34 BDSG durch Inkassounternehmen

Auskünfte von Inkassounternehmen an Betroffene müssen vollständig sein.

Auch in diesem Berichtszeitraum beschwerten sich Betroffene über nicht erteilte Auskünfte nach § 34 BDSG durch Inkassounternehmen. Auf meine Intervention erteilten die verantwortlichen Inkassounternehmen die Auskünfte; dies jedoch in unvollständiger Weise: Im ersten Fall wurden Gläubiger- und Forderungsdaten nicht beauskunftet. Im zweiten Fall wurden die Gläubigerdaten unvollständig beauskunftet, die Forderungsdaten nicht beauskunftet und der Zweck der Speicherung nicht eindeutig genug bezeichnet.

Meine daraufhin durchgeführte Beratung der verantwortlichen Inkassounternehmen führte in einem Fall zu einer vollständigen und damit gesetzeskonformen Auskunftserteilung der betroffenen Person. In einem weiteren Fall sicherte mir das verantwortliche Inkassounternehmen zu, seine Datenübersichten entsprechend meinen Anregungen hinsichtlich der entsprechenden Daten zu erweitern und die betroffene Person vollumfänglich zu beauskunften.

Sehr positiv ist zu konstatieren, dass bislang jedes der verantwortlichen Inkassounternehmen meine Anregungen jeweils unverzüglich und in kooperativer Weise umsetzte.

Hinsichtlich der weiteren Einzelheiten zu den zu beauskunftenden Daten verweise ich auf meine Ausführungen im Rahmen meines 43. Tätigkeitsberichts (Ziff. 5.3.11).

4.2.6

Datenübermittlung durch Inkassounternehmen an Auskunfteien

Ein fehlerhafter Forderungsdatensatz eines Inkassounternehmens führte zu unrichtigen Daten bei einer Auskunftei und war bei beiden Stellen zu korrigieren.

Eine betroffene Person wandte sich an mich und beschwerte sich darüber, dass eine Auskunftei mit Sitz in Hessen unzutreffende Forderungsdaten in ihrem Datensatz zu dem Schuldner gespeichert habe. Ursächlich hierfür sei, dass ein bayerisches Inkassounternehmen zu zwei titulierten Forderungen, zu denen ein rechtskräftiges Urteil und ein Kostenfestsetzungsbeschluss vorlagen, wiederholt unzutreffende Titel- und Forderungsdaten an diese Auskunftei übermittelt habe.

Daraufhin ließ ich mir zu Prüfungszwecken die Datenübersicht der Auskunftei zu dem Schuldner sowie Kopien der vorbezeichneten Titel nebst den Forderungsaufstellungen des Inkassounternehmens vorlegen. Das Ergebnis meiner Prüfung bestätigte den Vortrag des Schuldners insofern, als das Inkassounternehmen die gegenständlichen Titel- und Forderungsdaten nicht korrekt in die Inkassosoftware eingepflegt hatte, was folglich zu einer Übermittlung teilweise unrichtiger Daten seitens des Inkassounternehmens an die Auskunftei führte.

Gemäß § 35 Abs. 1 BDSG sind personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

§ 35 Abs. 1 BDSG

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

Auf meine Intervention veranlasste das Bayerische Landesamt für Datenschutzaufsicht zuständigkeitshalber eine Korrektur der unrichtigen Daten in der Software des Inkassounternehmens sowie die Erstellung einer zutreffenden Forderungsaufstellung (§§ 366, 367 BGB). Aufgrund der Bereinigung des Forderungsdatensatzes der betroffenen Person ist künftig von einer korrekten Datenübermittlung durch das Inkassounternehmen an die Auskunftei auszugehen.

Bei der betroffenen Auskunftei veranlasste ich ebenfalls eine Korrektur des Datensatzes des Betroffenen.

4.3

Kredit- und Finanzwirtschaft

4.3.1

DS-GVO:

Vorbereitung auf das Wirksamwerden der Datenschutz-Grundverordnung im Bereich der Kreditwirtschaft

Durch umfangreiche Abstimmungen zwischen den Aufsichtsbehörden und mit den Verbänden der Kreditwirtschaft wurde die Anwendung der DS-GVO ab dem 25. Mai 2018 vorbereitet.

Mit der Ablösung des BDSG durch DS-GVO sind für die Kreditwirtschaft zahlreiche Rechtsunsicherheiten verbunden. Bisherige Datenverarbeitungsprozesse und Geschäftsprozesse sind zu überprüfen und in Frage gestellt. Durch einen intensiven Abstimmungsprozess zwischen den Aufsichtsbehörden und mit der Kreditwirtschaft konnte die Rechtsunsicherheit abgemildert werden. Dazu wurden einige als vordringlich bewertete Themen rechtlich geprüft und aufbereitet.

Dabei wurde Konsens erzielt, dass die bisher zulässigen Datenverarbeitungsprozesse der Kreditwirtschaft auch nach der DS-GVO weitgehend zulässig sein werden. Dies gilt insb. für die Verarbeitung von Daten aufgrund von bankaufsichtsrechtlichen oder anderen regulatorischen Vorschriften sowohl auf nationaler als auch auf europäischer Ebene. Der bisher zulässige Datenaustausch mit Auskunfteien kann zukünftig auf Art. 6 Abs. 1b und f DS-GVO gestützt werden.

Einwilligungen zur Datenverarbeitung sind jedoch an den Anforderungen der DS-GVO zu messen. Obligatorische Einwilligungen werden daher voraussichtlich nicht mehr zulässig sein. In der Regel kann die Datenverarbeitung und Datenübermittlung aber zukünftig auf die gesetzliche Grundlage des Art. 6 Abs. 1 DS-GVO gestützt werden. Dies gilt auch für den Verarbeitungsschritt des Profilings, der in der Regel aufgrund der Pflicht von Kreditinstituten zur Bonitätsprüfung aufgrund bankaufsichtsrechtlicher Vorschriften zulässig sein wird.

Durch die umfangreichen Abstimmungsverfahren und die damit verbundene Erzielung von Ergebnissen besteht im Tätigkeitsbereich der Kreditwirtschaft ab der Geltung des DS-GVO eine deutlich verbesserte Rechtssicherheit für betroffene Personen und die Wirtschaft.

4.3.2

Prüfungen von Unternehmen der Kreditwirtschaft

4.3.2.1

Prüfung von Kreditinstituten

Im Berichtsjahr habe ich verschiedene Kreditinstitute mit Sitz in Hessen geprüft. Hierbei habe ich lediglich in wenigen Fällen Beanstandungen aussprechen müssen.

Insgesamt wurden Datenerhebungs- und Datenverarbeitungsprozesse von 40 in Hessen ansässigen Kreditinstituten überprüft. Bei den Kreditinstituten handelte es sich um Sparkassen, Volksbanken sowie In- und Auslandsbanken. Schwerpunkte der Prüfungen waren die Rechtevergabe bezüglich der Zugriffe auf Kundendaten, Aufzeichnung von Telefonaten, Auskunfterteilung nach § 34 BDSG, Datenerhebung und -speicherung aus der Geschäftsbeziehung, Übermittlung von Daten an Auskunfteien, Mitarbeiterschulungen sowie die Auftragsdatenverarbeitung. Insgesamt ist festzustellen, dass in der überwiegenden Anzahl der Fälle seitens der Kreditinstitute eindeutig geregelt ist, wie bei den einzelnen Punkten zu verfahren ist. Die vorgelegten Arbeitsanweisungen erfüllten dabei größtenteils die datenschutzrechtlichen Anforderungen.

Dennoch gab es vereinzelt Grund zur Beanstandung. So wurde festgestellt, dass bei einer Vielzahl der geprüften Kreditinstitute eine Erhebung von Nutzerdaten über die Internetauftritte erfolgt, ohne den Betroffenen eine Möglichkeit einzuräumen, der Datenerhebung zu widersprechen. Hierbei bedienten sich die Unternehmen sogenannter Datenanalyse-Tools wie Piwik oder Google-Analytics. Nach § 15 Abs. 3 TMG ist es erforderlich, einerseits auf die Datenerhebung selbst sowie andererseits auf die Möglichkeit eines Widerspruchs hinzuweisen. Die Möglichkeit, der Datenerhebung zu widersprechen, kann mittels einer „Opt-Out-Funktion“ erfolgen. Bei einigen der geprüften Kreditinstitute fehlte hingegen diese Möglichkeit ganz oder aber boten diese keine funktionierende „Opt-Out-Verlinkungen“ auf deren Internetauftritten an.

Auch das Thema „Telefonaufzeichnungen“ nahm einen größeren Umfang in meiner Prüfung ein. In meinem 43. Tätigkeitsbericht (Ziff. 5.3.3) hatte ich meine Auffassung zu dem Thema „Aufzeichnung von Telefonaten bei Kreditinstituten“ bereits dargelegt. Dennoch habe ich feststellen müssen, dass Aufzeichnungen oftmals zu lange aufbewahrt werden. Auch erfolgten in einigen wenigen Fällen Aufzeichnungen von Telefonaten, ohne dass die entsprechenden Einwilligungen zur Aufzeichnung von den Betroffenen eingeholt wurden.

Positiv zu beurteilen ist, dass für alle in der Prüfung untersuchten Themen bei nahezu jedem Kreditinstitut umfangreiche Arbeitsanweisungen mit detaillierten Regelungen existieren. Auch hat meine Prüfung meine Ergebnisse aus dem Jahr 2014 bestätigt. In meinem 43. Tätigkeitsbericht (Ziff. 5.3.2) hatte ich bereits darüber berichtet, dass die geprüften Kreditinstitute angemessene Maßnahmen getroffen haben, um zu verhindern, dass Mitarbeiter ohne ausreichende Berechtigung auf die Daten ihrer Kunden zugreifen.

Insgesamt ist festzuhalten, dass ich lediglich in einem sehr geringen Ausmaß Verstöße gegen die Regelungen des BDSG festgestellt habe. Sämtliche Unternehmen haben auf meine Feststellungen hin die erforderlichen Maßnahmen eingeleitet, um eine datenschutzkonforme Datenerhebung und -verarbeitung sicherzustellen.

Aufgrund dessen, dass lediglich ein kleiner Teil der Datenerhebungs- und Datenverarbeitungsprozesse geprüft worden ist, werden sich auch in Zukunft weitere Prüfungen zu anderen Themen im Sektor Kreditinstitute anschließen.

4.3.2.2

Prüfungen von Bankfilialen

Bei der Durchführung der DS-GVO hat jede Aufsichtsbehörde für ihre durchgeführten Prüfungen einen hohen Grad an Nachvollziehbarkeit zu gewährleisten. Deshalb habe ich neben der beschriebenen Umfrage-Prüfung ein Prüfkonzept entwickelt, das eine Prüfung von Filialen vor Ort gestattet. Ziel der Prüfung muss ein allgemeinverständliches dokumentiertes

Ergebnis sein. Zu diesem Zweck wurde ein Fragenkatalog erstellt, der auch protokollarisch Notizen erlaubt.

4.3.2.2.1

Rahmenbedingungen

Der Schutz der monetären Transaktionen in ihren dazugehörigen jeweiligen Rechenzentren liegt schon im eigenen Interesse der Banken. Dies gilt in besonderer Weise nicht nur im Hinblick auf die IT-Sicherheit, sondern auch für die damit verbundenen datenschutzrechtlichen Anforderungen.

Die betrieblichen Datenschutzbeauftragten (bDSB) sind bei Kreditinstituten auf Unternehmens- und nicht auf Filialebene angesiedelt. Deshalb entfällt eine Prüfung, ob ein betrieblicher Datenschutzbeauftragter nach § 4f Bundesdatenschutzgesetz (BDSG) bestellt wurde und ob dieser seinen Aufgaben (insbesondere Schulungsmaßnahmen) nach § 4g BDSG nachkommt. Der Fokus liegt nicht auf den IT-Infrastrukturen in den Rechenzentren, sondern auf den filialinternen Prozessen, die die Bankangestellten befähigen, datenschutzkonform mit personenbezogenen Daten ihrer Kunden umzugehen. Zudem sind die örtlichen Gegebenheiten zu berücksichtigen. Der Schwerpunkt der Prüfung liegt deshalb auf der Einhaltung der technischen und organisatorischen Maßnahmen (TOMs) in den Filialen auf Grundlage der Anlage zu § 9 BDSG. Im Zentrum einer solchen Prüfung vor Ort steht die Schaffung eines Bewusstseins, dass jede und jeder Angestellte für die Wahrung von Anforderungen des Datenschutzes mitverantwortlich ist. Die Ergebnisse dieser Prüfungen sollen dazu führen, die Filialleiterinnen und Filialleiter mit ihren Mitarbeiterinnen und Mitarbeitern zu befähigen, datenschutzkonform mit den personenbezogenen Daten ihrer Kundinnen und Kunden umzugehen.

4.3.2.2.2

Der Fragenkatalog

Um die Prüfung durchzuführen, ist eine Filiale zu besuchen. Daher ist auf Diskretion gegenüber den Kunden in der Filiale zu achten, insbesondere müssen deshalb Begehungen vor Ort während der Pausenzeiten stattfinden.

Ich habe einen Fragenkatalog entworfen, dessen Struktur sich an den technischen und organisatorischen Maßnahmen der Anlage zu § 9 Satz 1 BDSG orientiert:
- allgemeine Fragen zur Filiale,
- z. B. Zutrittskontrolle oder Zugangskontrolle wie auch Weitergabekontrolle und technische und organisatorische Maßnahmen bzgl. Papierakten und Datenträgervernichtung.

Entsprechende Beispiele sind:
- Aufstellung der Bankautomaten, mit denen die Kunden im „Self-Service“ ihre Bankgeschäfte erledigen, oder
- die Sicherung der Zugänge, insbesondere in geschützte Bereiche, in denen z. B. die Arbeitsplatzrechner der Mitarbeiterinnen und Mitarbeiter sich befinden.

Bei geprüften Filialen unterschiedlicher Banken ist die Professionalisierung oder auch Institutionalisierung von Fortbildungsmaßnahmen zu gewährleisten. Diese sind zwar üblicherweise auf Unternehmensebene geregelt, eine Prüfung, ob diese Fortbildungsmaßnahme in den Filialen ankommt, bleibt erforderlich. An einigen Stellen wird ein Zertifikat automatisiert erstellt, wenn die Mitarbeiterinnen und Mitarbeiter einen solchen Online-Lehrgang erfolgreich abgeschlossen haben. Die angebotenen Unterlagen im Intranet der jeweiligen Banken waren zumeist umfangreich. Jedoch wird es vielen Mitarbeiterinnen und Mitarbeitern hierdurch auch erschwert, richtige Antworten auf die möglichen datenschutzrechtlichen Fragen der Kundinnen und Kunden zu finden. Oftmals führt das dazu, dass die Mitarbeiterinnen und Mitarbeiter mittels der öffentlichen Webseiten beraten. Hintergrundinformationen über die technischen und organisatorischen Maßnahmen sind besser über das Intranet zu vermitteln, insbesondere wenn die Zusammenhänge zwischen Datenschutz und Datensicherheit erklärt werden.

4.3.2.2.3

Mögliche weitere Prüfungen

Nachdem ich die Pilotphase abgeschlossen habe, werde ich im Jahr 2017 durch eine Prüfreihe feststellen, wie hoch das Datenschutzniveau in den Filialen der Kreditinstitute ist. Stichprobenartig müssen Filialen unterschiedlicher Unternehmen und Organisationsformen landesweit ausgewählt und geprüft werden. Ich erwarte ein hohes Datenschutzniveau in den Filialen festzustellen. Falls sich diese Annahme nicht bestätigen lässt, werde ich die

Filialprüfungen ausweiten, um das Datenschutzniveau in den Unternehmen weiter zu verbessern.

4.3.3
Prüfung eines Bonussystems

Stützt eine verantwortliche Stelle die Verarbeitung von personenbezogenen Daten auf eine freiwillig zu erteilende Einwilligung und erweckt sie dabei unzweifelhaft den Eindruck bei betroffenen Personen, der Umfang der Verarbeitung könne durch die Einwilligung kontrolliert werden, bestimmt ausschließlich der Umfang der erteilten Einwilligung die Zulässigkeit der Verarbeitung.

Ich wurde vom Betreiber eines Bonussystems gebeten, dessen datenschutzrechtliches Konzept zu einem bereits außerhalb Hessens betriebenen Bonussystem zu überprüfen. Das Bonussystem sieht die Gewährung von Prämien für Umsätze mit den teilnehmenden Unternehmen vor. Die Verarbeitung der Umsatzdaten wird dabei auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG und den geschlossenen Teilnahmevertrag gestützt. Die Datenschutzhinweise begrenzen den Umfang der Verarbeitung und legen fest, dass die personenbezogenen Daten ausschließlich zur Bemessung der ausgelobten Prämien verarbeitet werden.

Darüber hinaus werden teilnehmende Personen in mehreren Stufen um Erteilung einer Einwilligung für die Verarbeitung der personenbezogenen Daten zu Zwecken personalisierter Werbung, der Markt- und Meinungsforschung und der werblichen Ansprache mittels unterschiedlicher Medien gebeten. Dabei wird der Eindruck erweckt, dass der Umfang der Verarbeitung der Daten zu diesen Zwecken von der erteilten Einwilligung abhängt. Eine Teilnahme an dem Bonusprogramm war ohne erkennbare Nachteile auch ohne Erteilung einer Einwilligung möglich.

Bei der Prüfung des Systems wurde jedoch deutlich, dass bei der Verarbeitung der Daten keine Differenzierung zwischen Personen, die eine Einwilligung erteilt haben und die diese verweigert haben, erfolgt. Vielmehr werden für beide Gruppen erheblich mehr Daten als für die Prämienberechnung erforderlich erhoben und ausgewertet. Dabei werden insbesondere die genutzten Filialen und die dort jeweils getätigten Umsätze erfasst. Bei Personen, die eine Einwilligung erteilt haben, hätte die Datenverarbeitung auf diese Einwilligung gestützt werden können.

Auch wenn ein Bonussystem nur dann überhaupt rentabel betrieben werden kann, wenn die erhobenen Daten inhaltlich ausgewertet werden, ist dies nicht zulässig. Wird eine betroffene Person um Erteilung einer Einwilligung gebeten und wird diese nicht erteilt, kann für die Verarbeitung der Daten nicht auf andere Rechtsgrundlagen zurückgegriffen werden. Den betroffenen Personen wird mit der Vorlage einer zu erteilenden Einwilligung suggeriert, mit der Erteilung oder Verweigerung den Umfang der Datenverarbeitung kontrollieren zu können. Folglich darf eine Verarbeitung, für die eine Einwilligung verweigert wurde, auch nicht stattfinden.

Ein Rückgriff auf andere Rechtsgrundlagen, wie z. B. § 28 Abs. 1 Satz 1 Nr. 1 BDSG, mag nach dem Widerruf einer vorher erteilten Einwilligung möglich sein. Dies kann insbesondere dann der Fall sein, wenn aufgrund der erteilten Einwilligung bereits mit der Verarbeitung der Daten begonnen wurde. Wird die Erteilung einer Einwilligung aber bereits zu Beginn einer Geschäftsbeziehung verweigert, hat die von der Einwilligung umfasste Datenverarbeitung auch dann zu unterbleiben, wenn auch eine Rechtsgrundlage in Betracht käme.

Das Bonussystem konnte daher in Hessen nicht betrieben werden.

4.4
Energieversorger und Verkehr

4.4.1
Auskunftsersuchen an Konzerndatenschutzbeauftragte

Die datenschutzrechtlichen Auskunftsersuchen müssen an die jeweiligen Konzernunternehmen als selbstständige Einheiten gerichtet werden. Bei Auskunftsersuchen an eine Konzerndatenschutzabteilung müssen die betroffenen Unternehmen oder zumindest der Kontext der Verarbeitung vorgetragen werden.

Auffällig oft in diesem Berichtszeitraum kam die Frage auf, ob bei pauschalen Auskunftsersuchen an die Konzerndatenschutzabteilungen deren Verpflichtung besteht, bei allen von ihnen vertretenen Tochterunternehmen nach den personenbezogenen Daten des Auskunftsberechtigten zu suchen. Die datenschutzrechtlichen Auskunftsersuchen wurden in diesen Fällen an die Konzerndatenschutzbeauftragten gerichtet, ohne die Tochtergesellschaft, von der eine Auskunft begehrt wird, genauer zu bezeichnen. Auf die Bitte des Konzerndatenschutzes, zu präzisieren, von welcher Gesellschaft oder in welchem

Kontext die Auskunft verlangt wird, wurde nur pauschal geantwortet, dass der Konzerndatenschutzbeauftragte eine Suche starten solle.

Der datenschutzrechtliche Auskunftsanspruch muss sich gegen die verantwortliche Stelle richten. Verantwortlich ist nach § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Während Konzerne sich als wirtschaftliche Einheit verstehen und dementsprechend agieren, ist für das Datenschutzrecht das einzelne konzerngebundene Unternehmen als juristische Person maßgeblich. Der Gesetzgeber hat sich deutlich gegen ein Konzernprivileg entschieden, das es erlauben würde, alle Konzerngesellschaften als eine einheitliche verantwortliche Stelle (Informationseinheit) zu sehen. Adressat datenschutzrechtlicher Vorschriften ist stets nur das einzelne Konzernunternehmen (einschließlich der Konzernmuttergesellschaft), nicht jedoch der Konzern selbst.

Umgekehrt bedeutet das aber auch, dass sämtliche Konzernunternehmen im datenschutzrechtlichen Verhältnis als „Dritte“ zueinander stehen und dass die Datennutzungen untereinander nicht zugerechnet werden können.

Damit kann die Auskunft nach § 34 BDSG nicht an einen „Konzern“ gerichtet werden, sondern nur an die einzelnen Unternehmen. Diese müssen grundsätzlich gesondert angeschrieben werden. Auch ein Auskunftsersuchen bei der Muttergesellschaft erfasst nicht den ganzen Konzern.

Die Existenz von konzernübergreifenden Datenschutzabteilungen mit einem Konzerndatenschutzbeauftragten ändert daran nichts. Ein Konzerndatenschutzbeauftragter wird von den einzelnen Konzernunternehmen zum betrieblichen Datenschutzbeauftragten bestellt. Dieser ist insofern mit einem externen Datenschutzbeauftragten vergleichbar, der mehrere Unternehmen vertritt. In diesem Fall besteht selbstverständlich keine Verpflichtung des externen Datenschutzbeauftragten bei einem an ihn gerichteten Auskunftsersuchen bei allen von ihm vertretenen Unternehmen nach den über den Auskunftsberechtigten gespeicherten Daten zu suchen.

Es besteht somit keine datenschutzrechtliche Verpflichtung der konzernverbundenen Gesellschaften bzw. der Muttergesellschaft bei Erteilung der Auskunft nach § 34 BDSG füreinander einzustehen.

4.4.2

Der Abgleich der Kundendaten mit europäischen Antiterrorlisten

Der Abgleich der Kundendaten mit europäischen Antiterrorlisten ist datenschutzrechtlich zulässig.

Bei mir sind Anfragen aus der Wirtschaft eingegangen, die die Frage zum Gegenstand hatten, ob und in welchen Konstellationen gegen datenschutzrechtliche Regelungen verstoßen wird, wenn ein Unternehmen seine Kundendaten mit europäischen Antiterrorlisten abgleicht. In den genannten Fällen forderte die Compliance-Abteilung den Abgleich aller Handelspartner. Die Datenschutzaufsichtsbehörden haben bis jetzt den flächendeckenden und systematischen Abgleich der Beschäftigtendaten mit den europäischen Antiterrorlisten mangels einer Rechtsgrundlage abgelehnt.

Der Abgleich der Kundendaten mit den Antiterrorlisten ist dann nicht zu beanstanden, wenn es dafür eine datenschutzrechtliche Verarbeitungsgrundlage gibt. Denn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

Europäische Verordnungen können als in der Bundesrepublik unmittelbar geltendes Recht (Art. 249 EG-Vertrag, Art. 288 AEUV, Art. 23 GG) solche datenschutzrechtliche, bereichsspezifische Rechtsvorschriften sein, die die Datenverarbeitung erlauben oder anordnen. Die Antiterrorverordnungen sind die VO (EG) 881/2002 (Al Qaida-Verordnung), VO (EG) 2580/2001 (Embargomaßnahmen zur Terrorismusbekämpfung) und VO (EU) 753/2011 (Afghanistan- oder Taliban-Verordnung). Sie verbieten geschäftliche Beziehungen zu den terrorverdächtigen Personen und Organisationen, die im Anhang an die Verordnungen aufgeführt und immer wieder aktualisiert werden. Unter das in den Verordnungen festgeschriebene Bereitstellungsverbot von Geldern, anderen Vermögenswerten und wirtschaftlichen Ressourcen an gelistete Personen fallen neben Warenlieferungen und Geldzahlungen auch Zahlung von Arbeitsentgelt, Übertragung von Forderungen, Dienstleistungen (Service-Wartungstätigkeiten) und Wissenstransfer. Die Mittel, die sich für die persönliche Verwendung und den persönlichen Verbrauch eignen, sind nicht von dem Begriff „wirtschaftliche Ressourcen” umfasst. Die Festsetzung der Sanktionen zur Ahndung von Verstößen gegen die Antiterrorverordnungen erfolgt durch das Außenwirtschaftsgesetz (AWG).

Aus den drei EU-Antiterrorverordnungen und den hierzu ergangenen Normen des Außenwirtschaftsgesetzes ist der Abgleich nach hiesiger Einschätzung zwingend erforderlich, um eine Strafbarkeit bzw. Verhängung des Bußgeldes auszuschließen. Allerdings verlangt das vom Bundesverfassungsgericht herausgearbeitete Bestimmtheitsgebot, dass die datenschutzrechtlichen Verarbeitungsgrundlagen so ausgestaltet werden müssen, dass das Ausmaß der zulässigen Verarbeitung aus der Verarbeitungsgrundlage erkennbar und bestimmbar ist. Dies wird im Falle der Antiterrorverordnungen vielfach verneint. Auch das vom Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) als zuständige Bundesoberbehörde veröffentlichte Merkblatt zu länderunabhängigen Embargomaßnahmen zur Bekämpfung des Terrorismus (http://www.ausfuhrkontrolle.info/ausfuhrkontrolle/de/arbeitshilfen/merkblaetter/merkblatt_ebt.pdf) oder andere Maßnahmen stellen nicht klar, wie mit dem Abgleichverfahren oder mit seinen Ergebnissen umzugehen ist. So bleibt es den Unternehmen selbst überlassen, wie sie die Einhaltung der Antiterrorverordnungen sicherstellen.

Wenn man dieser Ansicht zustimmt und die Antiterrorverordnungen mangels Bestimmtheit ihrer Regelungstiefe als Verarbeitungsgrundlage ablehnt, ist der Rückgriff auf den § 28 Abs. 1 Satz 1 Nr. 1 BDSG möglich.

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten dann zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Die Datenverarbeitung ist dann für die Begründung eines Schuldverhältnisses erforderlich, wenn damit festgestellt werden soll, ob ein Schuldverhältnis überhaupt begründbar ist. Ein Schuldverhältnis ist dann nicht begründbar, wenn seiner Begründung ein gesetzliches Verbot im Sinne von § 134 BGB entgegensteht.

Bei den Antiterrorverordnungen handelt es sich um Embargoverordnungen mit der Besonderheit, dass auch Personenembargos geregelt werden. Die Nichtbeachtung von Bereitstellungsverboten der Art. 2, 3 und 4 der Antiterrorverordnungen wird als Embargoverstoß behandelt (Merkblatt des BAFA „Länderunabhängige Embargomaßnahmen zur Terrorismusbekämpfung“, S. 10). Verstöße gegen das Embargo der Europäischen Gemeinschaft führen zu Nichtigkeit des Rechtsgeschäfts (Palandt 72. Auflage § 134 RdNr. 18). Die Kenntnis der Listung des Vertragspartners ist schon aus diesen Erwägungen für die Begründung des Schuldverhältnisses zwingend erforderlich.

Auch muss ein Unternehmer vor der Begründung eines Schuldverhältnisses im Stande sein, das geschäftliche Risiko des einzugehenden Schuldverhältnisses abzuschätzen. Die Lieferung der Ware an die gelistete Person könnte beispielsweise von den Zollbehörden, die stichprobenartig den Abgleich durchführen, gestoppt werden. Es besteht die Gefahr, dass die bis zur Lieferung getätigten Aufwendungen (Herstellungskosten) nicht ersetzt werden, weil es zu keiner Lieferung gekommen ist und deswegen kein/kein vollständiger Kaufpreis gezahlt wurde.

Außerdem stellt die Begründung einer schuldrechtlichen Forderung – zumindest soweit Leistung und Gegenleistung vereinbart sind – die Zurverfügungstellung eines wirtschaftlichen Vorteils im Sinne der Antiterrorverordnungen dar. Denn eine Forderung kann im Rechtsverkehr abgetreten, verkauft oder verpfändet werden und stellt damit einen Vermögenswert an sich dar. Der Vertragspartner muss die Möglichkeit haben festzustellen, ob er durch den Vertragsschluss eine sanktionsbewehrte Handlung vollzieht.

Überdies ist die tatsächliche Erfüllung eines Schuldverhältnisses – Lieferung einer Ware, Erbringung einer Dienstleistung oder Geldzahlung – an eine gelistete Person durch unmittelbar geltende Antiterrorverordnungen verboten.

Durch die Zuwiderhandlung werden die Straftatbestände und Bußgeldvorschriften der §§ 17 ff. AWG, 25g ff. KWG erfüllt. Es drohen Entziehung und Verfall von Handelsgütern (§ 20 AWG) oder Nichtberücksichtigung bei nationalen öffentlichen Aufträgen bei einer verhängten Geldbuße (§ 149 Abs. 2 Nr. 3 GewO). Außerdem kann die Bewilligung des Hauptzollamtes zu vereinfachten Zollverfahren (AEO-Zertifikat – Authorized Economic Operator) entzogen werden. Dies hat enorme Nachteile bis hin zum Verlust der Exportfähigkeit zur Folge. Angesichts dieser einschneidenden Sanktionen erscheint es als nicht vertretbar, die Erforderlichkeit des Abgleichs für die Durchführung eines Schuldverhältnisses zu verneinen.

Im Falle der Ablehnung der datenschutzrechtlichen Grundlage für den Abgleich ist zu berücksichtigen, dass sich die Wirtschaftsunternehmen, die den Abgleich durchführen, in die Gefahr bringen die datenschutzrechtlichen Buß- und Strafvorschriften zu verwirklichen. Führen sie keinen Abgleich mit den Terrorlisten durch, bringen sie sich in Gefahr, die

Sanktionen des Außenwirtschaftsgesetzes auf sich zu ziehen, ein Ergebnis, das in Anbetracht des Grundsatzes der Einheit der Rechtsordnung nicht befriedigen kann.

Die Einwände, die gegen den Abgleich ins Feld geführt werden – schwieriges und komplexes Entlistungsverfahren, unzureichende Rechtsschutzmöglichkeiten, Verletzung des Anspruchs auf rechtliches Gehör, schwerwiegende Folgen für die irrtümlich gelistete Personen – können in Anbetracht der unmittelbaren Geltung der Verordnungen bei der Diskussion um deren Beachtung von privaten Firmen keine Berücksichtigung finden. Die Lösungen für diese Fragestellungen müssen auf der europäischen Ebene durch den Gesetzgeber gesucht werden. Die durch die Berücksichtigung der Einwände entstehende Rechtsunsicherheit kann nicht auf dem Rücken der durch die Antiterrorverordnung Verpflichteten ausgetragen werden.

Im Ergebnis ist festzustellen, dass selbst wenn man die Antiterrorverordnungen als bereichsspezifische Verarbeitungsgrundlagen für den Abgleich ablehnt, der Abgleich auf § 28 Abs. 1 Nr. 1 BDSG gestützt werden kann.

Den anfragenden Unternehmen habe ich mitgeteilt, dass ich den Abgleich der Handelspartner mit den Antiterrorlisten für zulässig halte, und habe meine Unterstützung bei der Gestaltung des Abgleichverfahrens zugesagt.

4.4.3
Einsatz von Funkwasserzählern durch die Wasserversorgungsunternehmen

Das bereits in meinem 43. Tätigkeitsbeitrag (Ziff. 4.1.5.8) erörterte Thema der Einführung von per Funk auslesbaren Wasserzählern beschäftigte mich in diesem Jahr verstärkt. Dabei hat sich die Notwendigkeit gezeigt, meinen damaligen Beitrag zu vervollständigen und weiterzuführen.

Die öffentliche Diskussion dreht sich um die Erforderlichkeit der Schaffung einer formell-gesetzlichen Grundlage, auf die die Erhebung und Verarbeitung von Wasserverbrauchswerten für Abrechnungszwecke mithilfe der Funkwasserzähler gestützt werden kann. Eine solche Verarbeitungsgrundlage ist bereits im Wasserrecht vorhanden.

Datenschutzrechtliche Grundlage für die Erhebung und Verarbeitung von Wasserverbrauchswerten für die Abrechnungszwecke

Die öffentliche Wasserversorgung ist als Aufgabe der Daseinsvorsorge (§ 50 Abs. 1 WHG) den Gemeinden als eine Aufgabe im eigenen Wirkungskreis überantwortet (§ 30 Abs. 1 HWG). Die Gemeinden können die Wasserversorgung öffentlich-rechtlich (Satzung) oder privatrechtlich (Versorgungsverträge) ausgestalten. Die Versorgungsbedingungen können dabei auf der Grundlage von Art. 243 EGBGB durch Rechtsverordnung geregelt werden. Dies ist geschehen durch die Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser des Bundeswirtschaftsministeriums (AVBWasserV).

Die Wasserversorgungssatzungen und Versorgungsverträge müssen entsprechend den Bestimmungen dieser Verordnung gestaltet werden (§§ 1 Abs. 1, 35 Abs. 1 Satz 1 AVBWasserV).

Die AVBWasserV bestimmt, dass die Wasserversorgungsunternehmen die verbrauchte Wassermenge durch die Messeinrichtungen feststellen und dass sie Art, Zahl und Größe sowie Anbringungsort der Messeinrichtungen bestimmen (§ 18 Abs. 1 Satz 1 und Abs. 2). Die Messeinrichtungen werden vom Beauftragten des Wasserversorgungsunternehmens möglichst in gleichen Zeitabständen abgelesen (§ 20 Abs. 1). Das Entgelt wird nach Wahl des Wasserversorgungsunternehmens monatlich oder in anderen Zeitabschnitten, die jedoch zwölf Monate nicht wesentlich überschreiten dürfen, abgerechnet (§ 24 Abs. 1). §§ 18, 20, 24 AVBWasserV stellen eindeutig eine datenschutzrechtliche Grundlage dar, die Wasserverbrauchswerte – sogar monatlich – abzulesen und für Abrechnungszwecke zu nutzen. Die Ablesung der Wasserverbrauchswerte mithilfe der Funkwasserzähler anstatt der herkömmlichen Wasserzähler stellt eine Änderung des Erhebungs- bzw. Ableseverfahrens dar und ändert nichts an der Tatsache, dass §§ 18, 20, 24 AVBWasserV eine datenschutzrechtliche Grundlage für die Verarbeitung von Wasserverbrauchswerten bereithalten.

Für die Änderung der Erhebungsmodalität wird im öffentlichen Bereich keine neue datenschutzrechtliche Grundlage benötigt. Dies gilt auch dann, wenn die neue Erhebungsmodalität im Gegensatz zu der ursprünglichen automatisiert abläuft. Das Ablehnen der Existenz der datenschutzrechtlichen Grundlage für den Fall der Ablesung und Nutzung der Wasserverbrauchswerte mithilfe der Funkwasserzähler würde zum Ergebnis führen, dass auch beim Einsatz von herkömmlichen Wasserzählern die Wasserverbrauchswerte nicht verarbeitet werden dürften.

Notwendigkeit der Änderung der Wasserversorgungssatzung beim Einsatz von Funkwasserzählern zu Abrechnungszwecken

Auch die Ausgestaltung des Erhebungs- und Verarbeitungsverfahrens muss selbstverständlich den datenschutzrechtlichen Grundsätzen genügen. Zu den Erhebungsmodalitäten enthält AVBWasserV eine Regelung in § 18 Abs. 2 Satz 2, wonach die Art der Messeinrichtung durch die Wasserversorgungsunternehmen bestimmt wird. Von dieser Ermächtigung müssen die Gemeinden in ihrer gemeindlichen Wasserversorgungssatzung Gebrauch machen. In der Wasserversorgungssatzung müssen die Art der Messeinrichtung (§ 18 Abs. 2 Satz 2 AVBWasserV) und somit auch die Art der Erhebung von Wasserverbrauchswerten festgelegt werden. Dabei müssen die Wasserversorgungsunternehmen den Stand der Technik bei der Entscheidung berücksichtigen und im Sinne der Sparsamkeit der Ressourcen handeln (§ 36 Abs. 1 Nr. 1, 4 HWG, § 50 Abs. 3, 4 WHG). Die hessischen Gemeinden haben mehrfach vorgetragen, dass die von ihnen eingesetzte Technik den jetzigen Standards entspricht und im geringeren Maße manipulierbar ist. Auch die genauen Ablesezeiten müssen angesichts der Tatsache, dass die Ablesung mithilfe der Funkwasserzähler für den Betroffenen nicht erkennbar ist, zum Zwecke der Transparenzschaffung in der Wasserversorgungssatzung unter Angabe des genauen Ablesedatums bestimmt werden.

§ 36 HDSG schreibt für die Nutzung von Datenverarbeitungs- oder Übertragungseinrichtung zum Zweck der ferngesteuerten Messungen oder anderer Wirkungen in Geschäftsräumen oder Wohnräumen eine Einwilligung des Betroffenen vor. Allerdings findet diese Vorschrift dann keine Anwendung, wenn bereichsspezifische Rechtsvorschriften eine datenschutzrechtliche Grundlage enthalten, die ferngesteuerte Messungen oder Wirkungen erlauben.

Eine solche bereichsspezifische Rechtsvorschrift stellt Art. 243 EGBGB, § 18 Abs. 2 Satz 2 AVBWasserV in Verbindung mit den Bestimmungen in den Wasserversorgungssatzungen dar.

Die Wesentlichkeitstheorie steht der Bestimmung der Art der Messeinrichtung in der Satzung nicht entgegen. Danach sind alle wesentlichen Entscheidungen – vor allem die Eingriffe in die Grundrechte – vom Gesetzgeber zu regeln. Hier geht es aber nicht um Schaffung einer datenschutzrechtlichen Grundlage durch die Satzung – diese ist in §§ 18, 20, 24 AVBWasserV geregelt –, sondern um die Ausübung der in der Bundesverordnung (§ 18 Abs. 2 Satz 2 AVBWasserV) vorgeschriebenen Befugnis, die Art der Messeinrichtung festzulegen. Damit sind die wesentlichen Anforderungen, nämlich die datenschutzrechtliche Grundlage und die Bestimmungsbefugnis über die Art der Messeinrichtung, schon in der auf der Ermächtigungsgrundlage des Art. 243 EGBGB erlassenen Bundesverordnung (AVBWasserV) geregelt.

Als Formulierungsvorschlag für Wasserversorgungssatzungen wird folgender Passus vorgeschlagen:

> „Die Gemeinde ermittelt die zur Verfügung gestellte Wassermenge durch Messeinrichtungen und bestimmt deren Art, Zahl und Größe sowie den Anbringungsort. Als Messvorrichtung werden die Funkmessgeräte installiert. Diese sind von den Gemeindebürgern zu nutzen. Die Gemeinde liest die Funk-Wasserzähler zu folgenden Zeitpunkten ab:
> (Genaue Benennung der Ablesezeiten bzw. ein Ableseplan)
>
> § 36 des Hessischen Datenschutzgesetzes findet aufgrund der anderweitigen Regelung keine Anwendung. Die Sicherheit der von Funkmessgeräten gesendeten Daten wird durch folgende Maßnahmen gewährleistet:
> (Aufzählung der konkreten technisch-organisatorischen Maßnahmen).“

Besonders hinweisen möchte ich darauf, dass meine Ausführungen lediglich die Verarbeitung von für Abrechnungszwecke erforderlichen Daten betreffen. Die Erhebung und Verarbeitung von zusätzlichen Daten für andere Zwecke mithilfe der Funktechnik bedarf besonderer Untersuchung. In letzter Zeit haben mich Anfragen hessischer Gemeinden erreicht, ob die eingesetzte Funktechnik auch für das Auffinden von Leckagen und Feststellung von Rückflüssen wie auch in Fällen des Manipulationsverdachts genutzt werden kann. Dies muss noch von mir im Einzelnen geprüft werden.

Die allgemeinen technischen Anforderungen an die eingesetzten Funkwasserzähler

Die technischen Anforderungen habe ich bereits in meinem 43. Tätigkeitsbericht wie folgt formuliert:

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

– Die Datenübertragung muss verschlüsselt erfolgen. Üblicherweise werden bei der Produktion der Zähler bereits Schlüsselwerte fest einprogrammiert.
– Es dürfen nur dazu vorgesehene Lesegeräte die Zähler auslesen können. Lesegeräte benötigen die zu den Zählern passenden Schlüssel.
  Es müssen kundenspezifische, oder eventuell sogar gerätespezifische, Schlüssel vergeben werden. Dies ist bereits bei der Produktion der Zähler zu beachten.
– Jeder Lesevorgang muss auch bei identischen Zählerständen zu unterschiedlichen Kryptogrammen führen.
  Wenn die rechtlichen und technischen Anforderungen erfüllt sind, ist ein datenschutzkonformer Einsatz von Funk-Wasserzählern gegeben. Die kommunalen Wasserwerke habe ich im Rahmen meiner Beratung dabei unterstützt, einen datenschutzgerechten Einsatz der Funk- und Wasserzähler sicherzustellen.“

Aus den vorliegenden Eingaben und der öffentlichen Berichterstattung wird jedoch deutlich, dass insbesondere die eingesetzte Verschlüsselungstechnik zwischen Funkwasserzählern und den Ablese-Empfängern zu Irritationen führt.

Zur Klarstellung sei hier nochmals ausgeführt, dass es bei Nutzung von asymmetrischen Schlüsselpaaren im Unterschied zu symmetrischen Schlüsseln kein Problem ist, wenn alle Funkzähler eines Versorgers die Messdaten mit dem gleichen (öffentlichen) Schlüssel des Versorgers verschlüsseln. Wie bei einem entsprechend funktionierenden E-Mail-System ist dann nur der Versorger (Empfänger der Daten), der den dazu passenden (privaten) Schlüssel hat, in der Lage die chiffrierten Daten zu entschlüsseln und weiterzuverarbeiten.

Selbstverständlich kann ein Wasserversorger z. B. für verschiedene Versorgungsbereiche unterschiedliche Schlüsselpaare einsetzen, um die Folgen eines Verlustes des privaten Schlüssels zu minimieren. Gerät der private Schlüssel durch den Diebstahl mobiler Endgeräte oder durch einen Hackerangriff auf das Versorgungsunternehmen in falsche Hände, ist der Wasserversorger dazu verpflichtet, die öffentlichen Schlüssel an den Funkwasserzählern auszutauschen bzw. zwischenzeitlich das Funkmodul der Zähler zu deaktivieren.

Wichtig ist bei der Verwendung asymmetrischer Schlüsselpaare, dass sowohl die Wasserversorger als auch die Hersteller der Geräte sicherstellen, dass der private Schlüssel eines Schlüsselpaares immer nur einem Wasserversorger „ausgeliefert“ wird, damit eine versorgerübergreifende Entschlüsselungsmöglichkeit ausgeschlossen bleibt.

4.4.4
eTicket Rhein-Main des RMV

Zum 01.01.2016 wurde beim RMV das eTicket als verpflichtendes Medium nicht nur für den Erwerb von Jahreskarten, sondern auch für Zeitkarten (Wochen- und Monatskarten) an Automaten oder im Vertrieb über Geschäftsstellen eingeführt. Die Ausgabe als Papierfahrschein ist bei Wochen- und Monatskarten nur noch ausnahmsweise, beispielsweise in Bussen, möglich.

In meinem 40. Tätigkeitsbericht (Ziff. 3.5.1) für das Jahr 2011 hatte ich über die Einführung des eTickets durch den RMV berichtet. Das eTicket ist als deutschlandweiter Standard für elektronische Fahrscheine konzipiert und hat als Trägermedium eine Chipkarte. In der Endausbaustufe soll es möglich sein, deutschlandweit Fahrscheine aller Verkehrsunternehmen mit einem einzigen eTicket zu erwerben.

Neben der Möglichkeit, Fahrscheine vollständig anonym zu erwerben, als sogenannte „white card“, ist die Möglichkeit der Personalisierung gegeben. Diese ist teilweise für den Erwerb von vergünstigten und personengebundenen Fahrscheinen aber erforderlich (z. B. Jobticket).

In diesem Jahr habe ich die Abläufe bei Kontrollen und beim Ersatz eines eTickets geprüft.

4.4.4.1
Umfang der Prüfung

Mit einer anonymen Fahrkarte habe ich im Rahmen eines Versuchs die wesentlichen Nutzungsmöglichkeiten mit dem Ziel durchgespielt, die mit der Fahrkarte durchgeführten Aktionen im Hintergrundsystem des RMV zu überprüfen, zu verifizieren und mit den auf dem eTicket gespeicherten Daten abzugleichen.

Dies waren im Einzelnen
– Beschaffung einer Chipkarte (am Kundenschalter der DB)
– Anonymer Erwerb einer Fahrkarte (an einem DB-Automaten)

- Durchführung von Kontrollen während der Nutzung bei verschiedenen Verkehrsunternehmen
- Sperren des Fahrscheins (Verlust)
- Beschaffung einer Ersatzfahrkarte

Mit frei verfügbaren Apps aus dem Google-Playstore ist es möglich, die auf der Chipkarte gespeicherten Transaktionen mit Hilfe eines NFC-fähigen Smartphones nachzuvollziehen. Diese gespeicherten Transaktionen habe ich im Rahmen des Versuches ausgelesen und mit den Daten des Hintergrundsystems beim RMV verglichen. Ferner habe ich mir anhand vorhandener Kartennummern von Mitarbeitern meiner Dienststelle mit deren Einverständnis die im Hintergrundsystem vorliegenden Daten angesehen.

4.4.4.2

Datenspeicherung auf der Chipkarte und im vHGS, Kontrolldatensätze

Spezifikation eTicket

Neben der Ausgabe von Fahrscheinen sieht die Spezifikation des eTickets vor, dass optional Kontrollen mit geeigneten Lese- (und Schreib-)Geräten auf der Chipkarte gespeichert werden können. Hierfür ist ein Ringspeicher mit zehn Einträgen vorgesehen (d. h., der 11. Schreibvorgang löscht den ältesten Eintrag: Eintrag 1 fällt weg, Eintrag 2 wird Eintrag 1 usw. Eintrag 10 ist dann neu und gleichzeitig der aktuellste).

Hier habe ich im Rahmen des Versuches verschiedenste Einstellungen vorgefunden – teilweise sogar innerhalb eines Verkehrsunternehmens abhängig vom Kontrollgerät.

Beispiele:

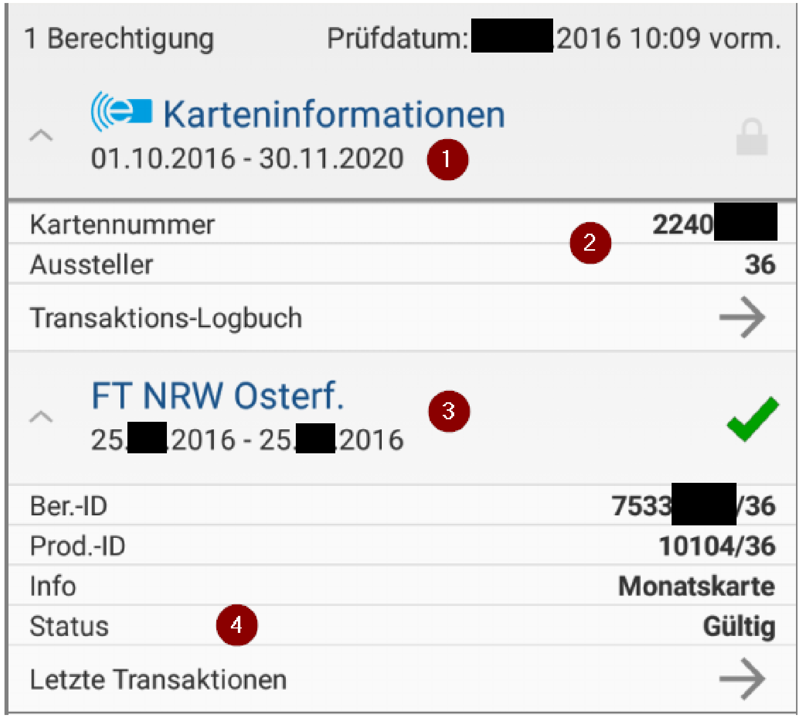
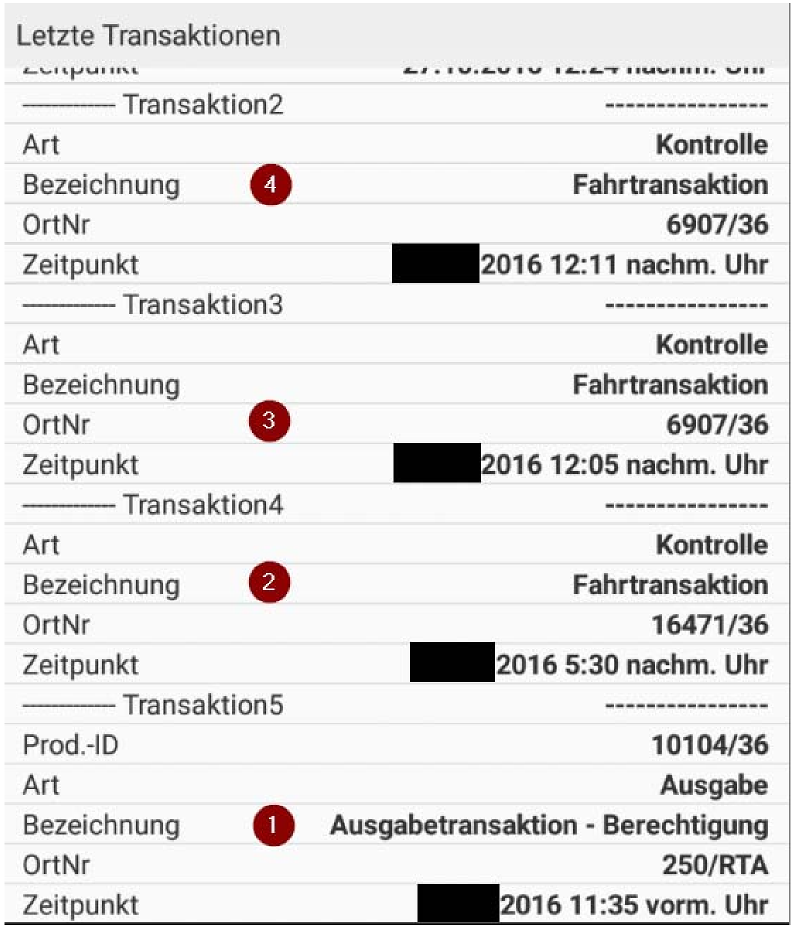

1 Berechtigung
Prüfdatum: [redacted] 2016 10:09 vorm.
Karteninformationen
01.10.2016 - 30.11.2020
Kartennummer 2240[redacted]
Aussteller 36
Transaktions-Logbuch
FT NRW Osterf.
25[redacted]2016 - 25[redacted]2016
Ber.-ID 7533[redacted]/36
Prod.-ID 10104/36
Info Monatskarte
Status Gültig
Letzte Transaktionen

Bild 1 – Karten- und Fahrscheininformationen

Erläuterungen
1 Informationen zur Gültigkeit der Karte
2 Allgemeine Karteninformationen
3 Informationen zum Fahrschein (lt. Informationen der App, die in diesem Fall eine Monatskarte der ESWE darstellt)
4 Status des Fahrscheins



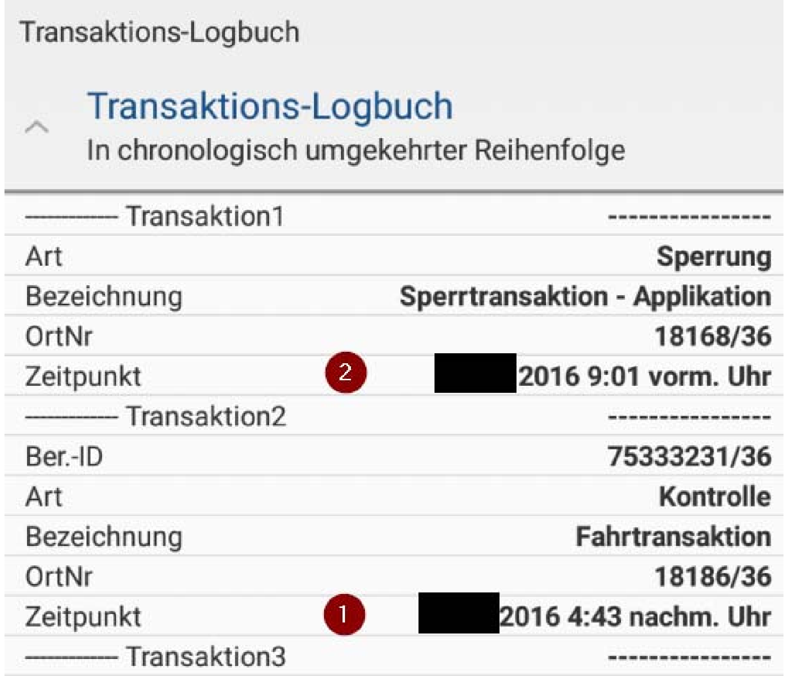
Letzte Transaktionen

---------- Transaktion2	----------------
Art	**Kontrolle**
Bezeichnung ④	**Fahrtransaktion**
OrtNr	**6907/36**
Zeitpunkt	[redacted] **2016 12:11 nachm. Uhr**
---------- Transaktion3	----------------
Art	**Kontrolle**
Bezeichnung	**Fahrtransaktion**
OrtNr ③	**6907/36**
Zeitpunkt	[redacted] **2016 12:05 nachm. Uhr**
---------- Transaktion4	----------------
Art	**Kontrolle**
Bezeichnung ②	**Fahrtransaktion**
OrtNr	**16471/36**
Zeitpunkt	[redacted] **2016 5:30 nachm. Uhr**
---------- Transaktion5	----------------
Prod.-ID	**10104/36**
Art	**Ausgabe**
Bezeichnung ①	**Ausgabetransaktion - Berechtigung**
OrtNr	**250/RTA**
Zeitpunkt	[redacted] **2016 11:35 vorm. Uhr**

Bild 2 – Ringspeicher mit Transaktionseinträgen

Erläuterungen

1	Erwerb des Fahrscheines (Ausgabetransaktion) an einem Fahrkartenautomaten
2 bis 4	Kontrollen während der Fahrt



Transaktions-Logbuch

Transaktions-Logbuch
In chronologisch umgekehrter Reihenfolge

---------- Transaktion1	----------------
Art	**Sperrung**
Bezeichnung	**Sperrtransaktion - Applikation**
OrtNr	**18168/36**
Zeitpunkt ②	[redacted] **2016 9:01 vorm. Uhr**
---------- Transaktion2	----------------
Ber.-ID	**75333231/36**
Art	**Kontrolle**
Bezeichnung	**Fahrtransaktion**
OrtNr	**18186/36**
Zeitpunkt ①	[redacted] **2016 4:43 nachm. Uhr**
---------- Transaktion3	----------------

Bild 3 – Sperrinformation

Erläuterungen

1	Letzte Kontrolle
2	Sperreintrag nach gemeldetem Verlust der Karte bei der nächsten Kontrolle

Hintergrundsystem des RMV

Das Hintergrundsystem des RMV (vHGS, verbundweites Hintergrundsystem) sammelt täglich von allen teilnehmenden Verkehrsunternehmen (VU) die Informationen ein, die diese vorab von ihren mobilen und stationären Geräten (Fahrscheinautomaten, Kontrollgeräte) gesammelt haben. Diese Daten werden weiterverarbeitet und die relevanten Daten werden nachts an die VUs zurückübertragen. Diese spielen die Daten wieder in ihre Automaten und Kontrollgeräte ein, sodass sie am nächsten Tag verfügbar sind.

Die wesentlichen Daten, die von den VUs an das vHGS übertragen werden oder im vHGS eingetragen sind:

- Ausgabe von Fahrscheinen
- Kontrolldatensätze

– Neue Sperraufträge für Karten und erfolgte Sperrungen

Die nächtliche Datenübermittlung vom vHGS umfasst insbesondere alle offenen Sperraufträge und Fahrscheine, die noch nicht auf dem zugehörigen eTicket gespeichert werden konnten. Dies bedingt beispielsweise, dass die Information über die Sperre anderen Geräten erst am Folgetag zur Verfügung steht. Wird die Karte danach kontrolliert, liegt im Kontrollgerät ein Sperrdatensatz vor, der sofort auf die Karte übertragen wird.

Mit diesen Informationen über den Fahrschein habe ich mir das Hintergrundsystem des RMV angesehen und versucht, die von der Chipkarte bekannten Informationen nachzuvollziehen und festzustellen, was dort an weitergehenden Informationen gespeichert ist.

Als Suchkriterien dienen die Nummer der Chipkarte sowie die Nummer des Fahrscheins, der dem Ausgabebeleg zu entnehmen ist. Diese Informationen benötigt ein Kunde bei anonymen Fahrkarten, wenn er im Verlustfall einen Ersatz erhalten will. Deshalb empfehlen VUs die Daten bzw. Belege aufzubewahren bzw. zu notieren.

Schwerpunkt meiner Prüfung war der Umgang mit Kontrolldatensätzen; nachfolgend ein Beispiel der im vHGS gespeicherten Kontrolldatensätze:

```
Fahrttransaktion[
  allgemeineTransaktionsdaten=AllgemeineTransaktionsdaten[
    logApplikationSeqNummer=SequenceNumberTwo[4]

logNmTransaktionID=NmTransaktionID[samSequenznummer=SequenceNumberFour[35
2],samID=SAMNumber[samNr=ReferenceNumberThree[2***6]]]
    logTransaktionsOperatorID=ReferenceNumberTwo[6**6]

logTerminalID=TerminalID[terminalTyp=TerminalTypCODE[code=15,msg=Fahrerte
rminal (Verkauf und
Kontrolle)],terminalNummer=ReferenceNumberTwo[3**7],terminalOwnerID=Organ
isationID[orgaNr=ReferenceNumberTwo[6**6]]]

logTransaktionsZeitpunkt=DateTimeCompact[date=DateCompact[**.**.2016],tim
e=TimeCompact[12:**:42]]
    logTransaktionsOrtID=OrtID[ortTyp=OrtsTypCODE[code=2*3,msg=Im
Fahrzeug der
Haltestelle.],ortNumer=ReferenceNumberThree[6**7],ortDomaeneID=Organisati
onID[orgaNr=ReferenceNumberTwo[36]]]
    logTransaktionsTypCode=NmTransaktionstypCODE[code=27,msg=Kontrolle]
  ]

transaktionProduktspezifischerTeil=TransaktionProduktspezifischerTeilRMVE
FS[
  ]
  allgemeineFahrttransaktionsdaten=AllgemeineFahrttransaktionsdaten[

berBerechtigungId=BerechtigungID[berechtigungNummer=ReferenceNumberFour[7
****231],kvpID=OrganisationID[orgaNr=ReferenceNumberTwo[36]]]

berLogFahrtID=FahrtID[fahrtBetreiberID=OrganisationID[orgaNr=ReferenceNum
berTwo[36]],fahrtNummer=ReferenceNumberThree[7*]]

berLogLinieVarianteID=LinieVarianteID[linieID=ReferenceNumberTwo[2*],vari
antenNummer=ByteU[0*]]
    berLogSeqNummer=SequenceNumberTwo[3]

fahrtabschnitttransaktionFahrtbeginn=FahrtabschnitttransaktionFahrtbeginn
[berLogHaltestelleID=OrtID[ortTyp=OrtsTypCODE[code=0,msg=Bushaltestelle
(busStopStation
)],ortNumer=ReferenceNumberThree[0],ortDomaeneID=OrganisationID[orgaNr=Re
ferenceNumberTwo[0]]],berLogSeqNummerFahrtbeginn=SequenceNumberTwo[0],log
TransaktionsZeitpunkt=DateTimeCompact[date=DateCompact[01.01.1990],time=T
imeCompact[00:00:00]]]

fahrtabschnitttransaktionVorgaenger=FahrtabschnitttransaktionVorgaenger[b
erLogHaltestelleID=OrtID[ortTyp=OrtsTypCODE[code=0,msg=Bushaltestelle
(busStopStation
)],ortNumer=ReferenceNumberThree[0],ortDomaeneID=OrganisationID[orgaNr=Re
ferenceNumberTwo[0]]],logTransaktionsZeitpunkt=DateTimeCompact[date=DateC
ompact[01.01.1990],time=TimeCompact[00:00:00]]]

prodProduktId=EFMProduktID[produktNummer=ReferenceNumberTwo[1***4],pvID=O
rganisationID[orgaNr=ReferenceNumberTwo[36]]]
    macKontrolle=0000000000000000
    versionKKontrolle=00
  ]
]
```

Ergebnis der Prüfung Datenspeicherung, Kontrolldatensätze

Im Rahmen der Prüfung wurden alle relevanten Datensätze wiedergefunden; weitergehende Daten wurden nicht gefunden.

Die Speicherung von Kontrolldatensätzen im vHGS ist unter dem Aspekt der Missbrauchskontrolle durch die Unternehmen nachvollziehbar. Hiermit lässt sich z. B. feststellen, ob eine (gefälschte) Karte in engem zeitlichem Rahmen an geografisch weit entfernten Orten eingesetzt wurde, was nach einer Überprüfung zur Sperre führen kann.

Darüber hinausgehende Informationen – insbesondere Detailinformationen zur Fahrt (Linie und Fahrtrichtung) – sind in diesem Fall nicht erforderlich und dürfen unter dem Aspekt der Datensparsamkeit auch nicht erhoben werden; auch wenn die Spezifikation des eTickets diese vorsieht.

Im Rahmen der Prüfung ist dies aufgefallen. Der RMV hat mir umgehend zugesichert, die Applikation dahingehend anzupassen, dass diese Informationen zukünftig nicht mehr in den Kontrolldatensätzen gespeichert werden.

Mittlerweile hat der RMV auch die Möglichkeit geschaffen, als Kunde in einer personalbedienten RMV-Vertriebsstelle mit eTicket-Akzeptanzsymbol die auf der Chipkarte gespeicherten Datensätze einzusehen und löschen zu lassen.

4.4.4.3

Ausstellung einer Ersatzkarte

Ich habe auch den Verlust einer Chipkarte samt Sperrung und Beschaffung einer Ersatzkarte mit Ersatzfahrschein getestet. Die Chipkarte war eine „white card“ und die Monatskarte war an einem Automaten gekauft und bar bezahlt worden; der RMV und die VUs hatten daher keine Daten über mich als Kunden.

Bei der Verlustmeldung wurde zuerst nach der Chipkartennummer gefragt. Diese ist auf der Chipkarte aufgedruckt und auf dem Begleitbrief, der bei der Ausgabe einer Chipkarte dem Kunden ausgehändigt wird. Ohne Kenntnis der Kartennummer kann nicht gesperrt werden. Für die Sperre wird zusätzlich die Quittung vom Kauf der Monatskarte benötigt; der Ausdruck wird beim Kauf optional angeboten. Auf der Quittung befindet sich die Nummer der Fahrkarte. Nur wenn – wie in meinem Fall – Chipkartennummer und Fahrkartennummer bekannt sind und nach den Daten im vHGS zusammenpassen, kann man eine „white card“ sperren lassen. Nachdem ich die erforderlichen Angaben gemacht hatte, wurde für meine Karte eine Sperre eingetragen. Bei einer personalisierten Fahrkarte, d. h., im vHGS sind Daten zur Person des Kunden, zu seiner Chipkarte und zu seiner Fahrkarte gespeichert, kann man sich durch einen Ausweis legitimieren und die Sperre vornehmen lassen.

Nach der Eintragung der Sperre bekam ich problemlos eine Ersatzmonatskarte für den verbleibenden Gültigkeitszeitraum der ursprünglichen Monatskarte. Die Daten im vHGS zu diesem Vorgang stimmten mit den Daten auf der Chipkarte überein. In meinem Fall war immer noch nicht bekannt, welcher Kunde die (Ersatz-)Monatskarte erhalten hat.

Abhängig von den Gründen für die Sperre und Ausstellung einer Ersatzkarte können Gebühren anfallen.

Ergebnis Ausstellung einer Ersatzkarte

Die Abläufe entsprachen den Angaben in den AGBs. Bei Verlust konnte auch eine anonyme Zeitkarte ersetzt werden und der Kunde war für den RMV und das VU weiterhin anonym. Es wurden keine weiteren Daten erhoben.

4.4.4.4

Zusammenfassung

Die Datenverarbeitung des RMV entsprach den vertraglichen Vorgaben. Es ist möglich, das eTicket anonym zu nutzen. Durch die jetzt jedem Kunden offenstehende Möglichkeit, die Kontrolldatensätze auf der Chipkarte löschen zu lassen, werden seine Interessen noch besser berücksichtigt.

4.5

Versicherungswirtschaft

4.5.1

Datenverarbeitung in der Versicherungswirtschaft mittels Auskunfteien

In der Versicherungswirtschaft hat es datenschutzrechtliche Fortschritte gegeben. Der Datenaustausch zwischen den Versicherern bewegt sich mittlerweile auf einem datenschutzrechtlich akzeptablen Niveau bzw. die weitere Entwicklung geht unter Begleitung der Datenschutzaufsichtsbehörden dort hin.

In der Versicherungswirtschaft gibt es jedenfalls seit den 1990er Jahren Bestrebungen, das Versicherungsrisiko mit Blick auf den Vertragsabschluss durch Informationsaustausch der Versicherer untereinander solide einschätzen zu können und die Vermeidung von Leistungsmissbrauch/Versicherungsbetrug branchenweit (und nicht nur durch jeden Versicherer in Eigenregie) anzustreben. Dies geschah zunächst ohne datenschutzrechtliche und insbesondere auch ohne datenschutzaufsichtsbehördliche Steuerung. Zunehmend wurde aber der versicherungsbrancheninterne Informationsaustausch [Stichworte: Uniwagnis, altes HIS (Hinweis- und Informationssystem)] auch zu einem Datenschutzthema, was insbesondere an Mängeln betreffend die Transparenz des Verfahrens und die

Information der Betroffenen lag. Die weitere Entwicklung mündete 2011 in den Aufbau einer Auskunftei im Sinne des Bundesdatenschutzgesetzes (§ 29) und damit verbunden in eine deutliche Erhöhung der Transparenz und Stärkung der Betroffenenrechte. Dieses („neue“) HIS entstand durch Abstimmung des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) mit den Datenschutzaufsichtsbehörden. Die Auskunftei wird von der informa HIS GmbH betrieben, die ihren Sitz seit Juni 2015 in Wiesbaden hat und somit meiner Zuständigkeit unterfällt; neben der für die Kreditwirtschaft bedeutsamen Auskunftei SCHUFA, die ebenfalls in Wiesbaden betrieben wird.

Im Bereich speziell der Privaten Krankenversicherungswirtschaft ist die Entwicklung noch nicht so weit gediehen, aber sie bewegt sich dorthin. In dieser Sparte, die vom HIS nicht erfasst ist, gibt es zwar einen Informationsaustausch zwischen den Versicherern in Form von Umfragen; dieses Verfahren soll aber wie schon zuvor bei den anderen Versicherungssparten zukünftig ebenfalls im Wege einer Auskunftei betrieben werden. In diesem Sinne laufen zurzeit die Abstimmungen zwischen dem Verband der Privaten Krankenversicherer (PKV e. V.) und den Datenschutzaufsichtsbehörden (konkret: Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises).

Der weitere Fortgang wird ein Thema im nächsten Tätigkeitsbericht sein.

4.5.2
DS-GVO:
Verhaltensregeln (Code of Conduct) der Versicherungswirtschaft

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV, Berlin) passt die datenschutzrechtlichen Verhaltensregeln der Versicherungswirtschaft an die Vorgaben der DS-GVO an. Die Datenschutzaufsichtsbehörden begleiten diesen Prozess.

Verhaltensregeln als branchenspezifisches Datenschutzrecht

Ein Regelungsgegenstand der DS-GVO sind Verhaltensregeln (Art. 40). Insoweit knüpft die DS-GVO an die EG-Datenschutzrichtlinie von 1995 an (ausführlich hierzu etwa *Dammann/Simitis*, EG-Datenschutzrichtlinie, Kommentar, Erläuterungen zu Art. 27). Auf Art. 27 der EG-DR beruht der nachträglich in das BDSG aufgenommene Verhaltensregeln betreffende § 38a BDSG, der die gesetzliche Grundlage für den geltenden Code of Conduct (CoC) der Versicherungswirtschaft bildet. Solche Verhaltensregeln werden vom europäischen Datenschutzrecht als Regelungsinstrument positiv bewertet. Dies zeigt sich schon daran, dass es – wie auch schon in Art. 27 EG-DR – in Art. 40 DS-GVO auffordernd heißt, dass die Mitgliedstaaten die Ausarbeitung von Verhaltensregeln „fördern“.

> Art. 40 Abs. 1 DS-GVO
>
> Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Verarbeitungsbereiche ... zur ordnungsgemäßen Anwendung dieser Vorschrift beitragen sollen.

Der Aspekt der Überarbeitung/Änderung von bereits bestehenden Verhaltensregeln, hier: in Form des aktuellen CoC, wird anschließend in der Vorschrift in Absatz 2 angesprochen:

> Art. 40 Abs. 2 DS-GVO
>
> Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftraggebern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:
>
> a) faire und transparente Verarbeitung;
> b) die berechtigten Interessen des Verantwortlichen ...
> ...
> k) ...

Verfahrensrechtlich ist geregelt, dass Verbände und andere Vereinigungen, die beabsichtigen, Verhaltensregeln auszuarbeiten oder „bestehende Verhaltensregeln zu ändern“ oder zu erweitern, den „Entwurf zu deren Änderung oder Erweiterung“ der Aufsichtsbehörde vorlegen (Art. 40 Abs. 5 DS-GVO).

Dementsprechend hat der GDV signalisiert, dass er auch unter der Geltung der DS-GVO Verhaltensregeln als Instrument der Selbstregulierung beibehalten möchte. Deshalb besteht mit Blick auf die geltenden Verhaltensregeln Anpassungsbedarf.

Der derzeitige CoC ist von der Berliner Aufsichtsbehörde, der der Entwurf seinerzeit nach § 38a Abs. 1 BDSG „zu unterbreiten“ war, daraufhin überprüft worden, ob die „Vereinbarkeit ... mit dem geltenden Datenschutzrecht“ bejaht werden kann. Das war in erster Linie das BDSG. Diese Vereinbarkeit wurde von der Berliner Aufsichtsbehörde in Absprache mit den anderen Datenschutzaufsichtsbehörden festgestellt.

Der CoC bekommt durch die DS-GVO einen neuen Prüfungsmaßstab, dem der CoC mit Geltung der DS-GVO ab dem 25.05.2018 gerecht werden muss. Es ist dann zum Beispiel für das Hinweis- und Informationssystem der deutschen Versicherungswirtschaft (HIS, dazu vgl. Beitrag „Datenverarbeitung in der Versicherungswirtschaft mittels Auskunfteien“) nicht mehr ausschlaggebend, dass der das HIS betreffende Art. 14 des CoC mit dem BDSG vereinbar ist, sondern es ist nun zu klären, inwieweit die in Art. 14 getroffenen Regelungen der DS-GVO entsprechen.

Für die anderen Artikel des CoC gilt das entsprechend. Denn Art. 40 Abs. 5 S. 2 DS-GVO verfügt, dass die Aufsichtsbehörde eine Stellungnahme darüber abgibt, ob der Entwurf zu deren Änderung oder Erweiterung mit dieser Verordnung vereinbar ist. Die Aufsichtsbehörde genehmigt diesen Entwurf zu deren Änderung oder Erweiterung, wenn sie der Auffassung ist, dass er ausreichende geeignete Garantien bietet (näher hierzu etwa *von Braunmühl* in Plath, Kommentar BDSG und DS-GVO, Art. 40 Rdnr. 12 ff.).

Mit Art. 40 DS-GVO tritt auch inhaltlich eine europarechtliche Weiterentwicklung für Verhaltensregeln ein (hierzu etwa *Spindler*, Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO, ZD 2016, 407 ff.). In der EG-DR war das Thema Verhaltensregeln nämlich mit Blick auf deren inhaltliche Ausgestaltung nicht näher geregelt und daran anknüpfend in § 38a BDSG auch nicht.

Nunmehr werden inhaltliche Aspekte von Verhaltensregeln ausführlich und explizit, allerdings exemplarisch, nicht abschließend, genannt. Im Katalog (Art. 40 Abs. 2) wird Fairness und Transparenz bei der Datenverarbeitung als Wichtigstes und konsequent auch als Erstes ausdrücklich betont.

Erst anschließend werden in der Vorschrift dann die „berechtigten Interessen des Verantwortlichen“ genannt (hierzu EG 4, 47; *Ziegenhorn/von Heckel*, Datenverarbeitung durch Private nach der europäischen Datenschutzreform, NVwZ 2016, 1584 ff.; zur Bedeutung der Vertragsfreiheit der Versicherer mit Blick auf Art. 12 (19 Abs. 3) GG im Spannungsfeld zur informationellen Selbstbestimmung BGH Urt. v. 13.07.2016, IV ZR 292/14 = DuD 2016, 751 = r+s 2016, 472, 474 f.).

Insgesamt werden in Art. 40 Abs. 2 DS-GVO beispielhaft elf Themenfelder (a bis k) von Verhaltensregeln genannt, die u. a. Gegenstand des CoC sein könnten.

Der materiell-rechtlich geprägte Art. 40 Abs. 2 wird verfahrensrechtlich durch Abs. 4 ergänzt. Dieser Absatz legt fest, dass Verhaltensregeln Verfahren vorsehen müssen, die es der in Artikel 41 Abs. 1 genannten Stelle (also einer akkreditierten Stelle) ermöglichen, die obligatorische Überwachung der Einhaltung ihrer Bestimmungen seitens der Verantwortlichen oder der Auftragsverarbeiter, die sich zur Anwendung der Verhaltensregeln verpflichten, vorzunehmen. Hiervon unberührt bleiben die Aufgaben und Befugnisse der Aufsichtsbehörde.

Im nächsten Tätigkeitsbericht werde ich die Entwicklung hinsichtlich der Anpassung des CoC an die DS-GVO weiter beschreiben.

4.6
Unternehmen, Selbstständige und Werbung

4.6.1
Unvollständige Auskunft durch einen Adresshändler

Die Nutzung von Adressdaten für postalische Werbung ist auch ohne die Einwilligung der/des Betroffenen erlaubt, wenn bei der Ansprache zum Zweck der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Sind mehrere Datenlieferanten/Datenübermittler beteiligt, sind diese zu speichern und auf Nachfrage des Betroffenen zu benennen. Auch bei einem ausländischen Unternehmen ist die vollständige postalische Anschrift mitzuteilen.

Anlass

Eine Betroffene hatte postalische Werbung für ein Hörgerät erhalten. Ein Adresshändler A war auf dem Werbeschreiben als für die Nutzung der Daten verantwortliche Stelle benannt. Dorthin richtete die Betroffene ihr Auskunftsersuchen. In seiner Antwort teilte der

Adresshändler A mit, die Daten von einem weiteren Adresshändler B erhalten zu haben. Dieser wiederum verwies bezüglich der Datenherkunft auf ein Unternehmen in der Schweiz, das er mit einer Abteilung dieses Unternehmens benannte, und teilte eine dortige Postfachadresse mit. Das so bezeichnete Unternehmen war im Internet nicht auffindbar.

Rechtliche Bewertung

Vor dem Hintergrund des Transparenzgebotes aus § 28 Abs. 3 Satz 5 BDSG hatte ich zu prüfen, wer auf dem Werbeschreiben als für die Nutzung der Daten verantwortliche Stelle benannt werden muss.

Rechtsgrundlage der Datenverarbeitung zu Werbezwecken ist § 28 Abs. 3 BDSG. Da das Werbeschreiben durch einen Dienstleister im sogenannten Lettershop-Verfahren versandt wurde, ist § 28 Abs. 3 Satz 5 BDSG anzuwenden.

§ 28 Abs. 3 Satz 5 BDSG

Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist.

Damit ist der Dienstleister, hier der Adresshändler A, auf dem Werbeschreiben zu benennen, da er die für die Nutzung der Daten verantwortliche Stelle ist. Eine Nennung der Beteiligten der insoweit vorher gegebenen Datenübermittlungskette, wie hier vom Adresshändler B an Adresshändler A und im ersten Schritt den Schweizer Adresshändler, sieht § 28 Abs. 3 Satz 5 BDSG nicht vor.

Im Wege eines Auskunftsersuchens nach § 34 Abs. 1 BDSG kann der Betroffene dann beim Adresshändler A dessen Datenlieferanten/Datenübermittler Adresshändler B erfahren.

Adresshändler B wiederum muss die Datenquelle, das Schweizer Unternehmen, beauskunften. Dies folgt aus der Speicherverpflichtung des § 34 Abs. 1a BDSG in Verbindung mit § 28 Abs. 3 Satz 4 BDSG.

§ 34 Abs. 1a Satz 1 BDSG

Im Fall des § 28 Abs. 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen.

§ 28 Abs. 3 Satz 4 BDSG

Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Abs. 1a Satz 1 gespeichert wird.

Die verantwortliche Stelle ist als konkrete juristische Person bzw. Firma mit ladungsfähiger Anschrift zu nennen. Kurzbezeichnungen (wie XY-Group) oder Postfachanschriften genügen dem Gesetzeszweck nicht. Dies gilt auch für ausländische Unternehmen (vgl. Nr. 3.12 der Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten für werbliche Zwecke, Stand Sept. 2014). Daher habe ich gegenüber dem Adresshändler beanstandet, dass er in der Auskunft nur die Abteilung des ausländischen Unternehmens und eine Postfachanschrift genannt hat. Die Adresse und der korrekte Name des ausländischen Unternehmens wurden dadurch verschleiert, sodass es der Beschwerdeführerin nicht möglich war, das Unternehmen aufzufinden.

Zurzeit wird im Rahmen eines Bußgeldverfahrens geprüft, ob ein Verstoß gegen § 43 Abs. 1 Nr. 8a BDSG vorliegt.

§ 43 Abs. 1 Nr. 8a BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
...
8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

4.6.2

Unverschlossenes Aktenlager eines Steuerberaters

Während einer Beratung bin ich im Rahmen einer Begehung des Kellers in einem Bürogebäude mit mehreren Mietparteien auf ein unverschlossenes Aktenlager eines Steuerberatungsbüros gestoßen. Es existieren zwar organisatorische Anweisungen für die Büroangehörigen, der Vorfall zeigt aber erneut, dass diese für den ordnungsgemäßen Umgang – insbesondere bei Akten mit erhöhtem Schutzbedarf – nicht immer ausreichen.

Bei der Begehung eines Kellers mit Aktenlagern verschiedener Mietparteien fand ich ein unverschlossenes Aktenlager eines Steuerberaterbüros vor. Das Bürogebäude selbst ist verschlossen und nur nach Anmeldung bei einer der Mietparteien über ein Treppenhaus zugänglich. Das Kellergeschoss kann nur über eine separate Treppe betreten werden, die lediglich von den abgetrennten Mietetagen erreichbar ist.

Damit erscheint zunächst für die Aktenlager im Keller ein ausreichender Zugangsschutz vorhanden zu sein. Der Vorfall zeigt aber, dass dieser nicht immer sichergestellt ist, zumal Angestellte einer anderen Mietpartei und deren Besucher, Handwerker und Mitarbeiter der Hausverwaltung (z. B. Hausmeister oder Reinigungskräfte) in der Regel unbeschränkte Zutrittsmöglichkeiten zu den Kellerräumen haben.

Wie mir die Kanzlei glaubhaft versicherte, besteht die grundsätzliche organisatorische Anweisung, das Aktenlager nach Abschluss der Tätigkeiten sofort wieder zu verschließen. Über die Vergabe der Schlüssel ist ein ordnungsgemäß geführtes Schlüsselbuch vorhanden. Allein darüber kann aber nicht sichergestellt werden, dass die angeordneten Maßnahmen immer ordnungsgemäß befolgt werden (Unachtsamkeit, Ablenkung, Praktikanten oder neue Mitarbeiter, die mit den Büroabläufen nicht bzw. noch nicht vertraut sind, usw.).

Dabei lässt sich diese Problematik durch einfache bauliche Veränderungen in Form eines Türknaufes und ggf. eines Türschließers bereinigen. Auch wenn der Raum nicht abgeschlossen ist, kann er nach Anbringung eines Türknaufs durch Unbefugte von außen nicht mehr geöffnet werden. Durch einen automatischen Türschließer kann zusätzlich sichergestellt werden, dass die Tür auch bei eiligem Verlassen des Raumes nach kurzer Zeit verschlossen ist (zu beachten ist hierbei allerdings, dass zur Umgehung des Türschließers gerne Keile genutzt werden). Ob weitergehende Maßnahmen wie Alarmanlage oder Bewegungsmelder, die sicherlich bei einem Mietgebäude eine Abstimmung mit dem Vermieter erfordern, sinnvoll sind, hängt von den jeweiligen Anforderungen ab. Insbesondere ist dabei zu berücksichtigen, dass diese Schutzmaßnahmen eher zur Einbruchssicherung vorgesehen sind und daher während der üblichen Bürozeiten oft ausgeschaltet werden bzw. aufgrund der regelmäßigen Personaltätigkeiten nicht immer überwacht und beachtet werden.

Das Steuerberaterbüro hat mir zwischenzeitlich nachweislich dargelegt, dass entsprechende bauliche Veränderungen an der Tür zum Aktenlager veranlasst wurden.

4.6.3

Anlassbezogene Außenprüfung bei einem Wirtschaftsunternehmen

Eine aufgrund von mehreren Beschwerden durchgeführte Datenschutzprüfung bei einem Unternehmen offenbarte gleich eine Reihe von Missständen.

Durch verschiedene Eingaben wurde ich darauf aufmerksam gemacht, dass Teile des Kundendatenbestands eines Unternehmens in einem im Ausland gehosteten Internet-Blog veröffentlicht worden waren. Zum Zeitpunkt der Eingabe waren die Kundendaten, unter denen sich auch Transaktionsdaten (allerdings ohne Bankverbindungsdaten) befanden, noch öffentlich abrufbar. Nachdem das Unternehmen auf die Veröffentlichung der Daten hingewiesen wurde, wurden die Einträge in dem Blog auf Geheiß des Unternehmens durch den Blog-Betreiber unkenntlich gemacht. Durch wen die Daten allerdings veröffentlicht wurden, konnte nicht sicher festgestellt werden. Problematisch erwies sich in diesem Zusammenhang, dass das Unternehmen auf Fristsetzungen zur Stellungnahme nicht reagierte. Auch von der Festsetzung eines Zwangsgeldes zeigten sich das Unternehmen sowie sein Rechtsbeistand unbeeindruckt. Daher erfolgte eine Vor-Ort-Prüfung des Unternehmens.

Es wurden Anhaltspunkte dafür gefunden, dass eine kürzlich aus dem Unternehmen ausgeschiedene Person weiterhin Zugriff auf die personenbezogenen Daten gehabt haben muss, da diese sehr wahrscheinlich für die Veröffentlichung der Kundendaten in dem Internet-Blog verantwortlich gewesen war. Es handelte sich dabei um die vormals mit der IT-Leitung beauftragte Person. Diese hatte sich selbst Berechtigungen eingerichtet, mit denen ein Zugriff auf die Daten des Unternehmens auch nach dem eigenen Ausscheiden noch möglich war. Zum Zeitpunkt der Vor-Ort-Prüfung durch den Hessischen Datenschutzbeauftragten hatte das Unternehmen bereits sämtliche Zugriffsmöglichkeiten durch die ehemalige IT-Leitung technisch unterbinden lassen.

Das Unternehmen hatte keinen Beauftragten für den Datenschutz bestellt, obwohl es nach § 4f Abs. 1 BDSG dazu verpflichtet gewesen wäre, da es sowohl automatisiert personenbezogene Daten verarbeitete als auch mehr als neun Personen ständig mit der Datenverarbeitung beschäftigte

§ 4f Abs. 1 BDSG

Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für die nicht-öffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. ...

Es wurde außerdem festgestellt, dass das Unternehmen ein anderes Unternehmen mit der Erhebung von Daten beauftragt hatte, ohne einen entsprechenden Vertrag über die Auftragsdatenverarbeitung geschlossen zu haben. Das beauftragte Unternehmen sollte für die Produkte des Auftraggebers werben und auf diesem Weg Kunden akquirieren. Nach § 11 Abs. 2 BDSG ist der Abschluss eines Vertrages in Schriftform allerdings zwingend erforderlich.

§ 11 Abs. 2 BDSG

Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist **schriftlich** zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

Nachdem ich die vorgenannten Verstöße gegenüber dem Unternehmen beanstandet habe, wurde sowohl ein Datenschutzbeauftragter bestellt als auch ein schriftlicher Vertrag zur Datenverarbeitung im Auftrag geschlossen.

Die Entscheidung über die Einleitung eines Ordnungswidrigkeitenverfahrens befindet sich derzeit noch in Prüfung.

4.6.4

Speicherung der Urlaubsanschriften von Zeitungsabonnenten

Wenn die Abonnenten von Tageszeitungen die Nachsendung der Zeitung z. B. an den Urlaubsort beauftragen, benötigen die Zeitungsverlage für die Zustellung die entsprechende Anschrift des Aufenthaltsortes. Nach Beendigung des kurzfristigen Aufenthalts und des Nachsendeauftrags ist es jedoch nicht mehr erforderlich, dass die Urlaubsanschriften dauerhaft vom Verlag gespeichert werden.

Eine Beschwerdeführerin, Abonnentin einer großen Tageszeitung, wollte sich beim Abonnentenservice telefonisch zu einem erteilten Nachsendeauftrag an den Urlaubsort erkundigen und stellte dabei fest, dass bei dem Zeitungsunternehmen sämtliche Adressen gespeichert waren, an denen die Betroffene in den vergangenen Jahren Urlaub gemacht hatte und an die sie sich die Zeitung hat nachsenden lassen. Da auch Anschriftendaten aus Nachsendeaufträgen gespeichert waren, die bereits viele Jahre zurücklagen, konnte das

Zeitungsunternehmen anhand dieser Daten über Jahre hinweg die Urlaubs- und Aufenthaltsorte der Abonnenten zurückverfolgen.

Auf meine Nachfrage hin wurde beim Zeitungsverlag schnell erkannt, dass die Speicherung der Nachsendeanschriften über einen derart langen Zeitraum nicht erforderlich ist. Allerdings können die Anschriftendaten auch nicht unmittelbar nach Beendigung des jeweiligen Nachsendeauftrages gelöscht werden. Soweit die Nachsendung der Zeitung ins Ausland erfolgt, ist diese kostenpflichtig. Bei der Beauftragung und Rechnungsstellung eines solchen Nachsendeauftrages werden beim Zeitungsverlag geschäftliche Unterlagen erzeugt, für die handels- und steuerrechtliche Aufbewahrungspflichten gelten. Die Nachsendung der Zeitung im Inland ist dagegen kostenfrei, so dass für einen solchen Auftrag keine besonderen Aufbewahrungsfristen bestehen. In beiden Fällen werden die Anschriftendaten des Nachsendeauftrages vom Verlag aber auch für die Bearbeitung eventueller nachträglicher Reklamationen der Abonnenten benötigt. Da solche zumeist in den ersten Wochen nach Beendigung des Nachsendeauftrages eingehen, ist die Aufbewahrung der Anschrift zu deren Bearbeitung zumindest für einen kurzen Zeitraum erforderlich.

Auf Anregung meiner Behörde wurde beim Verlag die Praxis bei der Speicherung von Nachsendeanschriften angepasst. Anschriftendaten aus Nachsendeanträgen ins Ausland werden seitdem ein Jahr nach deren Beendigung gelöscht. Auf diese Weise kann zwar der Auftrag zur Nachsendung noch belegt werden, soweit dies aus rechtlichen Gründen notwendig ist, es kann jedoch nicht mehr nachverfolgt werden, wohin genau die Zeitung nachgesendet wurde. Nach Ablauf der gesetzlichen Aufbewahrungsfrist werden die gesamten Informationen zum Nachsendeauftrag gelöscht. Bei Nachsendeaufträgen innerhalb des Inlandes werden die Adressdaten bereits einen Monat nach Ende der Nachsendung gelöscht, da nach diesem Zeitraum in aller Regel keine Reklamationen mehr erfolgen und die Daten auch nicht mehr zu anderen Zwecken benötigt werden.

4.7
Internet und Onlineshops

4.7.1
Internationale Datenschutzprüfung zum „Internet der Dinge“

Wie schon in den letzten Jahren hat der Hessische Datenschutzbeauftragte im Berichtszeitraum erneut am GPEN Internet Privacy Sweep 2016 teilgenommen. Bei dieser jährlich stattfindenden, internationalen Datenschutzprüfung wurden diesmal Dienste und Geräte aus dem Internet der Dinge untersucht. Bei der Prüfung der hessischen Anbieter standen besonders Geräte im Vordergrund, die unter dem Schlagwort „Smart Home“ vertrieben werden.

Immer mehr alltägliche elektrische Geräte erhalten heute „smarte“ Zusatzfunktionen, indem sie mit dem Internet verbunden werden und so z. B. eigenständig Informationen ermitteln und übertragen oder mit dem Smartphone ferngesteuert werden können. Zum sogenannten Internet der Dinge werden schon heute eine Vielzahl von Geräten gezählt wie z. B. intelligente Stromzähler, Thermostate, Smart-TV, Connected Cars oder Fitness-Tracker. Bei der Nutzung dieser Geräte werden fast immer auch personenbezogene Daten der jeweiligen Nutzer erhoben und verarbeitet. Dies hat das Global Privacy Enforcement Network (GPEN) zum Anlass genommen, bei einer internationalen Datenschutzprüfung Geräte aus dem Internet der Dinge zu untersuchen.

Das GPEN, ein informeller Zusammenschluss von Datenschutzbehörden aus der ganzen Welt, führt jedes Jahr eine Prüfungsaktion durch, in deren Rahmen die Beachtung des Datenschutzes bei Internetdiensten untersucht wird. Im Jahr 2016 haben dabei insgesamt 25 Datenschutzbehörden aus Europa, Nord- und Südamerika, Asien und Australien zusammen mehr als 300 Geräte und Dienste aus dem Internet der Dinge geprüft. Bei der Prüfung wurde vor allem untersucht, wie gut die Hersteller und Anbieter solcher Geräte ihre Kunden über die datenschutzrelevanten Aspekte ihrer Produkte informieren.

Der Hessische Datenschutzbeauftragte hat, wie auch in den letzten Jahren, an der Aktion teilgenommen und dabei seinen Fokus auf Dienste aus dem Bereich "Smart Home" gelegt. Darunter versteht man vor allem Haushaltsgeräte und Geräte aus dem Bereich Heimautomation, die mit dem Internet verbunden sind und so die Funktion verschiedener Anlagen im Haus (z. B. Licht, Heizung, Haushaltsgeräte, Sicherheitssysteme etc.) steuern.

Das Ergebnis der internationalen Prüfung zeigte, dass bei mehr als der Hälfte der Geräte im Internet der Dinge deren Nutzer nicht hinreichend darüber informiert werden, wie und wozu ihre personenbezogenen Daten erhoben, gespeichert und verarbeitet werden. Informationen dazu, wie die Nutzer ihre Daten wieder vom Gerät bzw. aus dem Dienst löschen können, wurden sogar nur bei weniger als einem Drittel der untersuchten Geräte und Dienste zur Verfügung gestellt. Erfreulicherweise wiesen die untersuchten Geräte und Dienste hessischer Anbieter keine gravierenden Datenschutzmängel auf. Dennoch war teilweise auch bei diesen Verbesserungsbedarf erkennbar, insbesondere was die Information der Nutzer angeht.

Das Internet der Dinge kann in vielen Lebensbereichen zu mehr Komfort und Sicherheit beitragen. Dies darf aber nicht zu Lasten des Persönlichkeitsrechts der Nutzer von intelligenten Geräten gehen. Die Hersteller und Anbieter von mit dem Internet verbundenen Geräten haben selbstverständlich das geltende Datenschutzrecht zu beachten. Dazu gehört es auch, die Nutzer darüber zu informieren, wie und zu welchen Zwecken ihre Daten erhoben und verarbeitet werden. Wenn die Nutzer befürchten müssen, dass sie von Geräten in ihrem Haushalt ausspioniert werden oder dass ihre Daten von den Anbietern nicht sorgfältig und sicher verarbeitet werden, wird möglicherweise die Akzeptanz der entsprechenden Geräte sinken.

4.7.2
Einbindung von Drittanbieter-Diensten auf Webseiten

Viele Webseitenbetreiber binden Dienste von spezialisierten Anbietern auf ihren Webseiten ein, um beispielsweise Werbeeinnahmen zu generieren, Informationen über die Nutzung der Webseite zu erhalten oder Inhalte in sozialen Netzwerken zu erzeugen. Viele dieser Dienste erheben und verarbeiten Daten der Webseitennutzer für ihre jeweiligen Zwecke. Die Betreiber der Webseite müssen ihre Nutzer daher auch über den Einsatz solcher Dienste informieren und ihnen die Möglichkeit geben, dem zu widersprechen.

Die meisten Webseiten bestehen aus einer Vielzahl von einzelnen Elementen wie z. B. Grafiken, Texten, Links, Werbebannern, Videos, Schaltflächen oder Social-Media-Buttons. Nur ein Teil dieser Bestandteile und Inhalte stammt vom eigentlichen Anbieter der Webseite, viele werden mittels Weblinks, Frames, Skripten und Plugins von anderen, auf bestimmte Dienste spezialisierten Anbietern geladen. Dies sind z. B. Werbenetzwerke, Analysedienste oder Social Networks. Bindet der Betreiber einer Webseite solche Dienste auf seinem Angebot ein, kann er auf diese Weise z. B. Werbeeinnahmen generieren oder Informationen über die Nutzung seiner Webseite erhalten. Der Webseitenbetreiber vermietet somit quasi Teile seiner Webseite an Dritte, die dort ihre eigenen Dienste anbieten, die teilweise den Nutzern, stets aber dem Betreiber der Webseite zugutekommen.

Die meisten dieser Dienste erheben und verarbeiten für ihre Zwecke Daten der Webseitennutzer, z. B. um diese bei einem erneuten Seitenaufruf wiedererkennbar zu machen (sog. Tracking), und unterfallen damit datenschutzrechtlichen Regeln. Die Anbieter von Webseiten, auf denen solche Dienste eingesetzt werden, sind deshalb gemäß § 13 Abs. 1 und § 15 Abs. 3 TMG dazu verpflichtet, die Nutzer auf die (zumeist im Hintergrund) stattfindende Datenverarbeitung hinzuweisen und eine Widerspruchsmöglichkeit gegen Tracking-Dienste zur Verfügung zu stellen.

Durch die Beschwerde eines Nutzers wurde ich auf die deutsche Webseite eines großen internationalen Unternehmens aufmerksam, die von dessen deutscher Niederlassung betrieben wird. Auf dieser wird eine Vielzahl von Drittanbieter-Diensten eingesetzt, vor allem Werbenetzwerke, Webanalyse-Dienste und Social-Plugins. Leider wurden dabei jedoch nicht im erforderlichen Umfang die datenschutzrechtlichen Anforderungen beachtet. So war für die Nutzer der Webseite weder erkennbar, welche Dienste von welchem Anbieter dort eingesetzt werden, noch wie deren Einsatz widersprochen werden kann. Die nur teilweise angebotenen Informationen und Widerspruchsmöglichkeiten waren dazu unzureichend. Für den Einsatz bestimmter Dienste waren zudem der Abschluss eines Vertrags mit dem Anbieter des Dienstes sowie bestimmte technische Anpassungen erforderlich, damit überhaupt eine Nutzung möglich ist, die den datenschutzrechtlichen Anforderungen gerecht wird.

Das Unternehmen wurde von mir aufgefordert und mit der Androhung von Zwangsmitteln dazu angehalten, entweder die festgestellten datenschutzrechtlichen Defizite auf der Webseite zu beseitigen oder die nicht datenschutzgerechte Nutzung von Drittanbieter-Diensten zu unterlassen. Daraufhin traf das Unternehmen die erforderlichen Maßnahmen, änderte die Datenschutzerklärung der Webseite, überarbeitete die gegebenen Widerspruchsmöglichkeiten und beseitigte die technischen und rechtlichen Defizite beim Einsatz bestimmter Dienste. So konnte letztlich erreicht werden, dass die Nutzer der Webseite nunmehr hinreichend darüber informiert werden, durch welche Dienste und zu welchen Zwecken ihre Daten verarbeitet werden und wie sie dem entgegentreten können. Zudem wurde sichergestellt, dass die eingesetzten Dienste nur im zulässigen Umfang und im Rahmen der rechtlichen Vorgaben genutzt werden.

Die Einbindung von Drittanbieter-Diensten auf den meisten Webseiten ist üblich und in vielen Fällen auch technisch und inhaltlich sinnvoll. Dabei darf von den Betreibern der Webseite jedoch nicht vergessen werden, dass sie datenschutzrechtlich auch für solche Dienste von Dritten mitverantwortlich sind und diesbezüglich eigene datenschutzrechtliche Anforderungen zu erfüllen haben. Dazu gehören insbesondere der Hinweis auf die Datenverarbeitung durch eigene und fremde Dienste auf der Webseite sowie das Angebot einer Widerspruchsmöglichkeit gegen Tracking-Dienste. Nur so haben die Nutzer die

Möglichkeit, sich über den Umfang der Verarbeitung ihrer Daten zu informieren und ggf. ihre Rechte geltend zu machen.

4.7.3

Zulässigkeit bzw. Unzulässigkeit der Zahlartensteuerung über Bonitätsanfragen bei Onlineshops

Eine Bonitätsanfrage bei Auskunfteien durch einen Onlineshop zur Steuerung der Zahlartenauswahl ist unzulässig. Erst nach Auswahl einer Zahlart mit „kreditorischem Risiko“ für den Händler ist die Einholung einer Bonitätsauskunft gerechtfertigt.

Im Rahmen einer Eingabe wurde festgestellt, dass ein Onlineshop verschiedene Zahlarten für seine Kunden anbietet. Es handelt sich hierbei um „Kauf auf Rechnung“, „Zahlung per Paypal“, „per Kreditkarte“, „per Geschenkkarte“ und „per Bezahldienst SOFORT Überweisung“. Der Auswahl der Zahlart (bis auf „Zahlung per Paypal“) vorgeschaltet war eine Bonitätsanfrage bei einer Auskunftei. Je nach Bonität wurden dem Kunden im Anschluss die dann möglichen Zahlarten als Auswahl zur Verfügung gestellt. Sofern eine schlechtere Bonität festgestellt wurde, bot der Händler als Konsequenz die Möglichkeit des „Kaufs auf Rechnung“ nicht mehr an.

Bei der Einholung einer Bonitätsauskunft bei einer Auskunftei handelt es sich um eine Datenerhebung. Diese ist nach § 4 Abs. 1 BDSG zulässig, wenn eine Rechtsvorschrift es erlaubt oder anordnet oder der Betroffene eingewilligt hat. In Betracht kommen die Regelungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, die es dem Händler gestatten, bei einem sogenannten „kreditorischen Risiko“ Daten zur Bonität des Kunden zu erheben. Das wäre dann der Fall, wenn der Händler wie beim Kauf auf Rechnung in Vorleistung geht. Ein derartiges Risiko liegt aber nur dann vor, wenn der Kunde eine entsprechende Zahlart auch tatsächlich nutzen möchte. Bei den im vorliegenden Fall angebotenen vier anderen Zahlarten ist ein „kreditorisches Risiko“ nicht gegeben, da die Zahlung entweder direkt erfolgt oder aber garantiert wird (Kreditkartenzahlung).

Eine Bonitätsprüfung zum Zwecke der Auswahl der Zahlart durch den Händler ist nicht erforderlich, da der Kunde möglicherweise gar nicht die Zahlart „Kauf auf Rechnung“ auswählen möchte. Für den Kunden ist es sicherlich unerfreulich, wenn er „Kauf auf Rechnung“ auswählt, ihm dann aufgrund der Ergebnisse der Bonitätsprüfung diese Zahlart verwehrt wird. Dennoch rechtfertigt das „Ersparen der Enttäuschung“, eine präferierte Zahlart doch nicht nutzen zu können, es nicht, eine Bonitätsanfrage ohne Erforderlichkeit dieser Datenerhebung vorzunehmen.

Problematisch ist auch, wenn der Bestellvorgang nach der Zahlartensteuerung abgebrochen wird, ohne dass eine Bestellung erfolgt. Letztlich besteht Grund zu der Annahme, dass die Betroffenen schutzwürdige Interessen an dem Ausschluss der Übermittlung haben. Es ist nicht auszuschließen, dass einige Auskunfteien die Anzahl der getätigten Bonitätsabfragen in ihre Scorewertberechnung einbeziehen. Daher könnte sich eine Bonitätsabfrage auf den Scorewert der Betroffenen auswirken.

Ich habe deshalb das Unternehmen aufgefordert, das Verfahren entsprechend den vorgenannten Anforderungen, umzugestalten. Dem kam das Unternehmen auch nach.

Nunmehr erfolgt erst dann eine Bonitätsabfrage, wenn der Kunde tatsächlich die Zahlart „Kauf auf Rechnung“ auswählt.

4.7.4

Prüfung eines Anbieters von Shopsystemen

Die Verarbeitung von Daten Dritter in einem Auftragsdatenverarbeitungsverhältnis ist nur zulässig, wenn eine angemessene Zugriffs- und Auftragskontrolle eingerichtet ist. Eine angemessene Zugriffskontrolle ist auch für interne Reportingsysteme einzurichten. Im Auftragsdatenverarbeitungsverhältnis ist die Nutzung von Daten durch den Auftragnehmer zu eigenen Zwecken nur zulässig, wenn dies dem Auftragnehmer durch den Auftraggeber gestattet wurde. Der Auftraggeber hat dabei die Rechte derer zu wahren, deren Daten verarbeitet werden.

Aufgrund einer Beschwerde bin ich auf ein Unternehmen in Südhessen aufmerksam geworden, das im Rahmen von Shopsystemen Daten im Auftrag von Kunden verarbeitet. Bei der durchgeführten Vor-Ort-Prüfung habe ich festgestellt, dass weder für den Zugriff auf die Systeme der Kunden noch für den Zugriff auf interne Reportingsysteme eine Zugriffskontrolle eingerichtet war. Ein Berechtigungskonzept mit Berechtigungs- und Rollenverwaltung existierte nicht. In alle Systeme war ein Login mit einem Single Sign-on mittels Namen und Passwort auch über einen Fernzugriff möglich. Weitere Sicherheitsmaßnahmen, wie beispielsweise VPN oder Code-Karten, wurden nicht genutzt. Nach dem Login konnte jeder Mitarbeiter auf alle Kundendaten uneingeschränkt zugreifen. Dies umfasste auch die Daten der betriebenen Shops und damit die dort getätigten Käufe der Kunden in den Shops des geprüften Unternehmens.

Sowohl die Daten der Shopsysteme als auch die eigenen Daten des Unternehmens, wie bspw. die Vertriebs- und Supporttätigkeit, wurden in einem umfassenden Reportingsystem erfasst und ausgewertet. Die Auswertungen wurden in einem Dashboard dargestellt, das für alle Mitarbeiter uneingeschränkt zugänglich war. Das Dashboard stellte auch die vertrieblichen Erfolge der Mitarbeiter personalisiert dar.

Eine Nutzungsberechtigung zur Nutzung der Kundendaten zu eigenen Zwecken des Auftragnehmers war in den Kundenverträgen nicht enthalten. Stattdessen hatten einige Kunden im Rahmen von Ergänzungsvereinbarungen klargestellt, dass es sich bei den verarbeiteten Daten um ihre Daten und die Daten ihrer Kunden handelt, die vom geprüften Unternehmen nicht verarbeitet werden dürfen.

Werden Daten verarbeitet, sind gemäß § 9 BDSG technische und organisatorische Maßnahmen zum Schutz dieser Daten zu treffen.

> § 9 BDSG
>
> Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Dabei sind gemäß Anlage zu § 9 Satz 1 BDSG unter anderem Maßnahmen zur Gewährleistung der Zugriffskontrolle und der Auftragskontrolle zu treffen.

> Anlage (zu § 9 Satz 1 BDSG)
>
> Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
>
> …
>
> 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
>
> …
>
> 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
>
> …

Durch eine angemessene Zugriffskontrolle ist zu gewährleisten, dass nur die Mitarbeiter auf die verarbeiteten Daten zugreifen können, die diesen Zugriff tatsächlich für ihre Tätigkeit benötigen. Dabei ist es nicht erforderlich, den Zugriff nur einzelnen Mitarbeitern zu gewähren. Durch angemessene Zugriffskonzepte können allen Mitarbeitern, deren Tätigkeit grundsätzlich einen Zugriff erfordert, entsprechende Rechte eingeräumt werden. Führt dies zu einer sehr großen Anzahl von zugriffsberechtigten Mitarbeitern, kann dies durch eine Protokollierung der Zugriffe und Überwachung der Mitarbeiter wieder ausgeglichen werden. Fehlt aber jegliche Zugriffskontrolle, wie dies hier der Fall war, stellt dies einen schwerwiegenden datenschutzrechtlichen Mangel dar.

Bei den in den Shops der Kunden des geprüften Unternehmens verarbeiteten Daten handelt es sich um Daten dieser Kunden. Diese sichern ihren Kunden – den Kunden der betriebenen Shops – die Einhaltung des Datenschutzes zu. Dazu gehört es auch, die Daten nicht an Unbefugte weiterzugeben. Die Beauftragung eines Dritten im Rahmen eines Auftragsdatenverarbeitungsverhältnisses ist dabei privilegiert. Die Datenverarbeitung im Auftrag stellt keinen Fall der Weitergabe von Daten dar, weil dem Auftragnehmer kein eigenes Recht zur Verarbeitung der Daten eingeräumt wird. Er darf die Daten gemäß § 11 Abs. 3 Satz 1 BDSG nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten und nutzen. Zur Auswertung der Daten zu eigenen Zwecken ist der Auftragnehmer daher nicht befugt. Dies gilt auch für eine anonymisierte oder pseudonymisierte Auswertung der Daten, weil bereits die Anonymisierung oder Pseudonymisierung der Daten eine Datenverarbeitung darstellt, die zulässig sein muss.

Dies war hier nicht der Fall. Weder hatten die Kunden des geprüften Unternehmens diesem ein entsprechendes Verarbeitungsrecht eingeräumt, noch wären sie dazu befugt gewesen.

Bei den betroffenen Daten handelt es sich um die personenbezogenen Daten von Kunden der Shops, die von einem Shopbetreiber angeboten werden. Den Shopbetreibern wird der Shop wiederum von dem geprüften Unternehmen in technischer Hinsicht zur Verfügung gestellt. Die Kunden der Shops begründen eine vertragliche Beziehung nur zu dem Shopbetreiber, der seinerseits eine vertragliche Beziehung zu dem geprüften Unternehmen begründet hat. In welchem Umfang die betroffenen Daten verarbeitet werden dürfen, richtet sich nach dem Verhältnis zwischen den Kunden der Shops und den Shopbetreibern. Diese sind ihrerseits nicht unbegrenzt berechtigt, die Daten an Dritte, wie das geprüfte Unternehmen, weiterzugeben. Vielmehr wird die Berechtigung zur Weitergabe durch die gesetzlichen Regelungen oder eine von den Kunden der Shops gewährte Einwilligung begrenzt. Ohne ausdrückliche Einwilligung dieser Kunden dürfen die Daten daher nur in dem Umfang verarbeitet werden, wie dies für die Ausführung der Bestellung erforderlich ist. Die Übermittlung der Daten an einen Auftragsdatenverarbeiter und die Einräumung eines eigenen Nutzungsrechts stellt keine für die Ausführung einer Bestellung erforderliche Datenverarbeitung dar.

Das Gleiche gilt für die unternehmensweite Verteilung der Daten von Beschäftigten. Auch deren Daten, z. B. die Dokumentation ihrer Tätigkeiten und Erfolge, dürfen gemäß § 32 Abs. 1 BDSG nur so weit verarbeitet werden, wie dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Die Weitergabe von Daten über Tätigkeiten einzelner Mitarbeiter über ein Dashboard gehört nicht dazu.

In das gesamte System war ein Login mittels Name und Passwort von beliebigen Endgeräten aus möglich. Eine vorherige Kontrolle der Integrität der Endgeräte erfolgte dabei nicht. Daher war es möglich, sich von Geräten mit installierten Viren, Trojanern und Keyloggern aus einzuloggen. Dadurch waren die gesamten Daten des kontrollierten Unternehmens und seiner Kunden stark und akut gefährdet. Zwar konnte ein entsprechender Zugriff nicht festgestellt werden. Dennoch sind derartige Sicherheitsmaßnahmen nicht mehr als ausreichend zu betrachten.

Das geprüfte Unternehmen hat die eigene Verarbeitung der Kundendaten unverzüglich gestoppt. Das Dashboard wurde umgehend abgeschaltet. Soweit darin Mitarbeiterdaten dargestellt wurden, wurde der Zugriff auf die Geschäfts- und Vertriebsleitung beschränkt. Eine solche Zugriffsbeschränkung ist datenschutzgerecht.

Zur Begrenzung des Zugriffs auf die Daten in den Shops entwickelt das Unternehmen ein angemessenes rollenbasiertes Zugriffskonzept. Bis zur Implementierung des Zugriffskonzeptes sind die Mitarbeiter angewiesen, auf die Daten nur in dem Umfang zuzugreifen, wie dies für ihre Tätigkeit erforderlich ist. Die Sicherheit des Fernzugriffs wird überprüft und geändert.

Die Fertigstellung aller erforderlichen Maßnahmen soll innerhalb einer angemessenen Frist von sechs Monaten erfolgen. Über die Maßnahmen erstattet das Unternehmen einen monatlichen Bericht.

4.7.5

Geolokalisierung vor der Newsletter-Versendung?

Der aufgekommene Verdacht, dass ein hessischer Immobilienmakler den aktuellen Aufenthaltsort von Internetnutzern und Newsletter-Empfängern ermittelt, um Inhalte seines Immobilien-Newsletters mit Haus- und Wohnungsangeboten individuell auf diese anpassen zu können, bestätigte sich nicht. Die aufenthaltsortsbasierte Individualisierung von Newsletter-Inhalten wäre datenschutzrechtlich unzulässig gewesen.

Wohnungs- und Immobilienangebote werden heute kaum noch in Printmedien veröffentlicht. Stattdessen finden sich immer mehr Angebote von Immobilienmaklern aus ganz Deutschland auf hierfür besonders spezialisierten Online-Marktplätzen, die von Wohnungssuchenden oder potentiellen Immobilienkäufern auch gerne und häufig genutzt werden. Diese Portale vereinfachen es Interessenten erheblich, in Frage kommende Häuser bzw. Wohnungen zu vergleichen, mit den anbietenden Maklern Kontakt aufzunehmen oder z. B. die Preisentwicklung in bestimmten Regionen, Ballungsräumen oder Marktsegmenten zu beobachten.

Einem Kaufinteressenten fiel allerdings auf, dass er, nachdem er über eine solche Online-Plattform bei einem hessischen Immobilienmakler sein Kaufinteresse für ein Haus in Köln geäußert und sich ein Exposé zu der Liegenschaft hatte zuschicken lassen, in der Folgezeit von diesem Unternehmen zwei Newsletter erhielt, die Angebote für genau die Städte oder Ballungsräume enthielten, in denen er sich kurz zuvor selbst aufgehalten hatte: Zuerst befand er sich beruflich in Frankfurt am Main, kurz darauf wurden im Newsletter des Maklers Immobilien in Frankfurt beworben. Danach weilte er im Urlaub im Salzburger Land und erhielt einen speziellen Newsletter mit Angeboten in Salzburg. Interesse an Häusern in Frankfurt oder Salzburg hatte er aber nie geäußert. Vor diesem Hintergrund befürchtete der Betroffene nun, dass der Immobilienmakler ermittelt, an welchem Ort er sich gerade befindet, wenn er ein Angebot des Maklers auf der Online-Immobilien-Plattform aufruft. Mit dieser Information über seinen Aufenthaltsort würde ihm der Makler dann entsprechend individualisierte und auf den Aufenthaltsort abgestimmte Immobilienangebote in dem Makler-Newsletter unterbreiten. Der Betroffene bat mich darum, die Sache aufzuklären und festzustellen, ob und gegebenenfalls wie der Makler den jeweiligen Aufenthaltsort seiner Online-Interessenten verfolgt und ob er aufgrund dieser Geolokalisierung seiner Newsletter-Empfänger eine individualisierte Anpassung der Newsletter-Inhalte vornimmt. Schließlich wollte er den Immobilienmarkt beobachten und nicht umgekehrt.

Jeder Internetnutzer geht mit einer ihm von seinem Zugangsprovider zugeteilten IP-Nummer ins Internet und hierlässt diese bei allen Anbietern der Dienste, die er nutzt. Da IP-Nummern durchaus einen Ortsbezug haben können, wäre es aus technischer Sicht möglich, dass der Makler anhand der dem Nutzer beim Aufruf des Internetangebots zugeordneten IP-Nummer versucht, eine grobe Lokalisierung des Nutzers vorzunehmen. Falls der Betroffene das Haus- und Wohnungsangebot mittels einer Smartphone-App der Immobilien-Online-Plattform aufruft, wäre auch eine Erhebung des GPS-Standortes des Nutzers durch diese App technisch machbar, wenn der Betroffene den GPS-Dienst an seinem Endgerät beim Aufruf des Immobilienangebots auf der Online-Plattform eingeschaltet hat. Sowohl bei IP-Nummern als auch bei GPS-Daten müsste die Online-Plattform mit den Immobilienangeboten diese Daten des Nutzers allerdings an den Makler übermitteln. Da der Betroffene angab, keine Immobilien-App zu benutzen und die GPS-Funktion seines Smartphones immer ausgeschaltet zu haben, blieb im vorliegenden Fall nur noch der Weg über die IP-Nummern-Lokalisierung.

Bei der IP-Nummer eines www-Nutzers handelt es sich um ein Nutzungsdatum. Aus datenschutzrechtlicher Sicht wäre die Verwendung dieses Nutzungsdatums durch einen Internetanbieter zu Lokalisierungszwecken allerdings unzulässig, da hierfür keine gesetzliche Rechtsgrundlage existiert. Das Telemediengesetz (TMG) erlaubt die Verarbeitung von Nutzungsdaten lediglich zur Diensteerbringung und zu Abrechnungszwecken:

§ 12 Abs. 2 TMG

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.

§ 15 Abs. 1 TMG

Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten).

Angesichts der Tatsache, dass bei stets weiter fortschreitender Technik die Methoden des Ortens, Verfolgens und Wiederkennens von Nutzern im Internet (sog. „User-Tracking“, „Targeting“ oder „Re-Targeting“) immer subtiler und ausgereifter werden und individualisierte Werbemaßnahmen generell weniger Streuverluste und mehr Erfolg versprechen als gleichlautende Massen-E-Mails habe ich den Immobilienmakler zur Stellungnahme zu den Befürchtungen des Nutzers aufgefordert. Zudem habe ich die dortigen Verfahren zur Zusammenarbeit mit der Online-Immobilien-Plattform sowie zur Erstellung und Versendung des Immobilien-Newsletters überprüft.

Bei dem Immobilienmakler handelte es sich um ein bundesweit tätiges Unternehmen mit vielen Standorten, das also auch ein entsprechend umfangreiches Portfolio an Immobilien betreut und bewirbt. Der Inhalt des Newsletters entspricht einer Auswahl an Immobilien dieses gesamten Portfolios. Die Auswahl der im Newsletter dargestellten Immobilien erfolgte auf rein redaktioneller Basis durch die Marketingabteilung des Unternehmens auf der Basis des vorhandenen Fachwissens über den Immobilienmarkt. Es waren dabei keinerlei statistische oder anderweitig gelagerte Programme oder programmähnliche Anwendungen, Automatismen oder Auswertungen im Einsatz.

Grundsätzlich sind Immobilien in größeren Städten oder Einzugsgebieten (z. B. Köln, Frankfurt, Rhein-Main-Gebiet, Salzburg) aus wirtschaftlichen Gründen immer geeigneter für die Darstellung in einem Newsletter, da sie für einen größeren Empfängerkreis interessanter sind als z. B. Immobilien im ländlichen Raum. Den speziellen Newsletter über den Standort Salzburg und den Newsletter mit dem Schwerpunkt Frankfurt hatten alle Newsletter-Empfänger gleichermaßen erhalten. Das bemängelte Muster stellte sich also als gar nicht so individuell heraus, sondern ließe sich auch mit anderen beliebigen Newsletter-Empfängern und anderen großen Städten wiederholen. Der Vermutung, dass hier eine vorherige Geolokalisierung eines Newsletter-Empfängers oder einer Gruppe dieser von dem Unternehmen Umworbenen stattgefunden habe, lag also tatsächlich ein missdeuteter Zufall zugrunde.

Und auch aus technischer Sicht konnte eine Geolokalisierung der Newsletter-Empfänger ausgeschlossen werden: Wenn eine Anzeige oder ein Angebot des Maklers über die Immobilien-Online-Plattform aufgerufen wird, müsste diese Plattform die IP-Nummer des Nutzers in irgendeiner Form zu Lokalisierungszwecken an den Makler übermitteln. Eine solche Übermittlung von IP-Nummern fand aber nicht statt. Wenn ein Kunde Interesse an einem Objekt bekundet, erhält der Makler von der Online-Plattform per E-Mail lediglich den Text der Anfrage und die vom Kunden angegebenen Kontaktdaten. Auch weitere technische Rahmenbedingungen des EDV-Systems und der Datenverarbeitungsprozesse lassen eindeutig den Schluss zu, dass von dem Makler weder eine IP-Nummer noch irgendwelche GPS-Daten oder andere ortungsfähige Daten für die Steuerung der Newsletter-Inhalte ausgewertet oder auch „nur“ erhoben und gespeichert werden.

Als Ergebnis meiner Nachforschungen konnte ich dem Betroffenen daher mitteilen, dass seine Befürchtungen und Ängste unbegründet waren. Ich habe in der Sache keine Anhaltspunkte dafür gefunden, dass der Immobilienmakler eine unzulässige Geolokalisierung seiner Kunden, Interessenten oder gar der Newsletter-Empfänger vornimmt. Es wurde kein Indiz für eine aufenthaltsortsbasierte Individualisierung der Newsletter-Inhalte entdeckt, die abgesehen von der klaren Rechtswidrigkeit ja auch recht aufwändig wäre. Es handelte sich bei dem, was der Betroffene als „auffällig“ wahrgenommen hatte, um einen gar nicht unwahrscheinlichen Zufall, welcher in keiner Weise mit irgendeiner Form von Geolokalisierung der Betroffenen stand.

4.7.6

Keine Löschung von Online-Kundendaten trotz Zusage

Wenn Betroffene ausdrücklich erklären, dass sie ein Online-Forum oder einen Online-Shop nicht mehr nutzen möchten, sind die personenbezogenen Daten in den Online-Kundenkonten zu löschen oder zu sperren. Regelmäßig wenden sich Betroffene an mich mit der Bitte, sie bei der Löschung ihrer Daten bei hessischen Online-Plattformen, -Foren und -Shops zu unterstützen.

Viele Internetnutzer legen im World Wide Web nach Interesse bei den unterschiedlichsten Online-Anbietern Kundenkonten, sog. „Online-Accounts“, an. Dies kann je nach Zweck und Ausrichtung der Online-Plattform und Erforderlichkeit für die Diensteerbringung unter Angabe weniger und eher unsensibler Daten geschehen, wie z. B. nur mit dem Nutzernamen, der E-Mail-Adresse und einem Passwort, wie es für das Login bei kommentierbaren Blogs oder in den meisten Hobby-Foren üblich ist. Im geschäftlichen Online-Bereich handelt es sich hingegen in der Regel um deutlich mehr und auch sensiblere Daten: Es werden Wohn- und Lieferanschriften, Geburtstag, Telefonnummer, Bankverbindung, Kreditkartendaten usw. erhoben. Falls es zum Kauf von Produkten oder Dienstleistungen kommt, liegen den Anbietern nach den ersten Online-Käufen auch die Daten zur Kauf- und Zahlungshistorie der Kunden vor.

Aus datenschutzrechtlicher Sicht ist die Speicherung dieser Daten durch die Online-Anbieter gemäß § 28 Abs. 1 Nr. 1 BDSG und § 14 Abs. 1 TMG dann zulässig, wenn ein Vertragsverhältnis besteht:

> § 28 BDSG
>
> (1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,
>
> 1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
>   ...
>
> § 14 Abs. 1 TMG
>
> Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten).

Mit dem Registrieren und Anlegen eines Online-Kundenkontos sind diese datenschutzrechtlichen Bedingungen des BDSG und des TMG für die Zulässigkeit der Verarbeitung der Nutzer- bzw. Kundendaten in der Regel erfüllt, wobei es gleichgültig ist, ob es sich bei der verantwortlichen Stelle um ein kostenloses Hobby-Forum handelt oder um einen Online-Anbieter, bei dem Produkte oder Dienstleistungen gekauft werden können.

Obwohl viele dieser Online-Konten oftmals nur ein einziges Mal benutzt werden, halten die Anbieter die Daten oft noch über viele Jahre vor. Zum einen, weil der Kunde aktiv einen Newsletter angefordert hat und man daher von weiterem Interesse ausgehen kann. Zum anderen auch nur, damit der Kunde sich bei einem nächsten Besuch nicht neu registrieren muss, sondern sich sofort bequem mit seinen noch gespeicherten Account-Daten als bekannter Bestandskunde online anmelden kann.

Wenn sich ein Betroffener aber entschließt, einen Online-Anbieter nicht mehr in Anspruch zu nehmen, nicht mehr in einem Forum mitzulesen oder sich an Diskussionen zu beteiligen oder nichts mehr in einem Online-Shop zu kaufen, ist der weiteren Speicherung seiner Daten durch den Anbieter damit die Rechtsgrundlage entzogen. Von einem Vertragsverhältnis bzw. einem rechtsgeschäftsähnlichen Rechtsverhältnis kann nach der Kündigung durch den Betroffenen nicht mehr ausgegangen werden. Alle dem Anbieter vorliegenden Daten des Betroffenen sind somit vollständig zu löschen. Diejenigen Online-Shop-Anbieter, bei denen Käufe getätigt oder kostenpflichtige Dienstleistungen in Anspruch genommen wurden, unterliegen allerdings den gesetzlichen Aufbewahrungspflichten der Abgabeordnung (AO) und des Handelsgesetzbuches (HGB) und dürfen die aufbewahrungspflichtigen Daten daher nicht löschen. Nach § 35 Abs. 3 Nr. 1 BDSG sind diese Daten zu sperren:

> § 35 Abs. 2 und 3 BDSG
>
> (2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn
> ...
> 3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder ...
>
> (3) An die Stelle einer Löschung tritt eine Sperrung, soweit
> 1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
>
> ...

Bei diesen Daten, die weiter gesperrt in den Archivsystemen vorgehalten werden müssen, handelt es sich in der Regel um Buchungsbelege über gewerbliche Einnahmen und Ausgaben aus dem kaufmännischen Buchungssystem des Online-Shops, die auch Daten von Käufern enthalten können. Die Zugangs- und Bestandsdaten aus dem Online-Account des ehemaligen Nutzers sind von diesen Aufbewahrungspflichten jedoch nicht betroffen. Diese personenbezogenen Daten sind daher gemäß § 35 Abs. 2 Satz 2 Nr. 3 BDSG vollständig zu löschen.

Zwar haben einige Anbieter ihren Kundenkonten mittlerweile Menüpunkte hinzugefügt, über die Nutzer eine Datenlöschung bzw. -sperrung selbst veranlassen können. Oftmals wird es den Nutzern aber eher schwer gemacht, eine vollständige Löschung bzw. Sperrung ihrer Daten zu erreichen. Auf Löschungsbitten über Online-Kontaktformulare wird selten reagiert, auf E-Mails an den Service mit Löschungsaufforderungen erhalten solche Kunden zwar manchmal automatisiert eine Ticketnummer des Shop-Service, aber dann keine weitere Antwort. Und selbst wenn die Datenlöschung im Online-Datenschutzhinweis ausdrücklich erwähnt und eine besondere Kontaktadresse hierfür angeboten wird, müssen Betroffene in der Praxis leider immer wieder feststellen, dass Anbieter ihren gegebenen Löschungszusagen nicht nachkommen. So werden z. B. nach angeblicher Datenlöschung weiterhin Newsletter versendet oder das Anmelden im Online-Konto ist dem Nutzer weiterhin möglich.

In allen Fällen, die Betroffene an mich herangetragen haben, wurden die jeweiligen Anbieter von mir unter Hinweis auf die Rechtslage zur Stellungnahme und zur Datenlöschung bzw. -sperrung aufgefordert. Die allermeisten Anbieter kamen meinen Aufforderungen umgehend nach. Als Erklärung für die rechtswidrige weitere Verwendung der Daten ehemaliger Kunden oder Nutzer entgegen deren Willen wurden zum Teil menschliche Fehler und mangelnde Sorgfalt von Mitarbeitern angegeben. Aber auch fehlerhaft definierte Geschäftsprozesse und mangelhafte technisch-organisatorische Maßnahmen für die Datenlöschung konnten als Gründe festgestellt werden.

So wurden im Falle eines gewerblichen Online-Shops zwar die Daten des Betroffenen aus den kaufmännischen Systemen gelöscht und gemäß § 35 Abs. 3 Nr. 1 BDSG gesperrt in die Archivsysteme der Stelle übertragen. Eine Löschungsbestätigung wurde versandt. Das Löschen der Daten des Online-Accounts (Name, E-Mail-Adresse, Passwort, Adressdaten) war damit allerdings nicht automatisch verbunden. Hierfür hätte es eines manuellen Eingreifens der Shop-Administration bedurft, was von einem dortigen Mitarbeiter aber übersehen wurde. Nach meiner Beanstandung wurde der Löschprozess im Unternehmen überarbeitet und vollständig automatisiert. Menschliche Fehler können so künftig weitgehend ausgeschlossen werden.

Bei einer Beschwerde gegen ein als Hobby betriebenes hessisches Kino-Online-Forum hatte ein Betroffener sein Löschungsersuchen an den Anbieter sowohl als E-Mail geschrieben als auch auf dessen privaten Anrufbeantworter gesprochen. Als dies nicht fruchtete, bat er den technischen Administrator des Kino-Forums per E-Mail um Datenlöschung. Dennoch erhielt er sogar immer weiter Newsletter des Anbieters mit Kino-Tipps. Bei meiner Nachfrage stellte sich heraus, dass dem verantwortlichen Anbieter und auch dem technischen Administrator letztlich gar nicht klar war, dass die datenschutzrechtlichen Regelungen des BDSG und des TMG auch für Hobby-Online-Foren gelten.

§ 2 TMG

Im Sinne dieses Gesetzes

1. ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält

...

§ 7 Abs. 1 TMG

Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

§ 3 Abs. 7 BDSG

Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt.

Es bedarf also keiner gewerblichen Tätigkeit, um den datenschutzrechtlichen Verpflichtungen aus diesen Gesetzen zu unterliegen. Hierfür genügt schon ein auf Dauer ausgerichtetes Angebot, bei dem personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Auch wenn der Anbieter und sein Administrator aufgrund anderer aktueller Verpflichtungen keine Zeit für das Forum und die Datenlöschung hatten, konnte ich sie überzeugen, kurzfristig ihre Prioritäten zu ändern und die gewünschte Datenlöschung umgehend zu vollziehen. Ich gehe davon aus, dass auch bei diesen hessischen Kino-Fans künftig eine höhere Sensibilität für datenschutzrechtliche Fragestellungen an den Tag gelegt wird.

In einem anderen Fall klagte ein Shop-Kunde darüber, dass ihm vom Shop-Service schon dreimal per E-Mail die Datenlöschung versprochen wurde, er aber immer noch Zugang zu seinem Online-Account hatte, seine Account-Daten also trotz mehrfacher Zusage nicht gelöscht wurden. Bei einer von mir deshalb veranlassten Überprüfung stellte sich heraus, dass der Nutzer in der Vergangenheit versehentlich zwei Kundenkonten angelegt hatte, die sich lediglich durch die Klein- bzw. Großschreibung eines Buchstabens in den Bestandsdaten des Nutzers unterschieden. Dass noch ein zweites Konto mit einem weiteren Kundendatensatz zum Betroffenen existierte, hatte das Unternehmen zuvor nicht bemerkt. Es erfolgte umgehend eine Löschung.

Über ein hessisches Hobby-Musik-Forum beklagte sich eine Betroffene, da der Anbieter sich weigere, ihre Anmeldedaten und ihren veröffentlichten Account mit Nutzername und Geburtsdatum zu löschen, obwohl sie das kostenlose Forum lediglich einmal vor vielen Jahren zu Recherchezwecken besucht habe und sich nur deswegen dort registriert habe. Eine Überprüfung ergab, dass der Anbieter wirklich in seinen Datenschutzhinweisen darüber informierte, dass erhobene Daten der Foren-Nutzer auf Dauer gespeichert und nie gelöscht werden. Nach mehreren Hinweisen auf die datenschutzrechtliche Unzulässigkeit seiner Datenverarbeitung und mit der Androhung eines Bußgeldverfahrens konnte der Anbieter zur Löschung der Daten der Beschwerdeführerin gebracht werden. Das Musik-Forum, in dem schon lange Zeit keine aktuellen Beiträge mehr von Nutzern eingestellt wurden, wurde von dem Anbieter inzwischen komplett aus dem Netz genommen.

4.7.7

Vorsicht vor Geldboten-Phishing

Auf zweifelhafte Angebote in unverlangt zugesendeten E-Mails darf nie eingegangen werden.

Auffällig war im Berichtsjahr der starke Anstieg der Eingaben zum sog. „Geldboten-Phishing“ (Phishing, aus dem Englischen – angeln). Dabei werden Betroffene per E-Mail aufgefordert, das eigene Konto für eine eingehende Überweisung zur Verfügung zu stellen, 80 % des Betrags an einen anonymen Empfänger weiterzuleiten und dafür den Rest als Provision einzubehalten. Der Aufwand würde vier bis acht Stunden pro Woche nicht überschreiten. Als Verdienst wurden zwischen 3.500 EUR und 4.400 EUR monatlich avisiert. Die Angebote klingen zunächst sehr lukrativ, da die geforderte Dienstleistung mit wenig Aufwand verbunden ist und verlockend gut bezahlt wird. Um frühzeitig das Vertrauen der Empfänger zu erwecken, wurde der E-Mail-Absender geschickt gefälscht und die E-Mail-Adresse einer in Hessen ansässigen großen Online-Jobvermittlungsplattform angegeben. Zudem enthielten alle mir von Betroffenen vorgelegten E-Mails den Namen, die Anschrift und die Telefonnummer der E-Mail-Empfänger. Die E-Mails waren also bemerkenswert hoch individualisiert, um sich von den leider seit Jahren üblichen und leichter erkennbaren Massen-Betrugs-E-Mails abzuheben und dem Empfänger zu suggerieren, dass es sich um ein attraktives Arbeitsangebot eines seriösen Anbieters handeln würde.

Einige Beschwerdeführer waren jedoch misstrauisch, da es sich bei genauerem Hinsehen um veraltete Daten zu ihrer Person handelte und sie zudem im Text dazu aufgefordert wurden, ihre „Bewerbung“ an eine ganz andere E-Mail-Adresse als an die angebliche Absender-Adresse zu schicken. Einige Betroffene beschwerten sich bei mir auch über die an der Versendung gar nicht beteiligte hessische Online-Arbeitsvermittlung, deren Adresse von den Betrügern als Absender gefälscht angegeben war.

Alle Eingeber wurden von mir darüber aufgeklärt, dass es sich bei diesen vermeintlichen Arbeitsangeboten um den Versuch handelt, Gehilfen zu finden, die von den Tätern zur Geldwäsche missbraucht werden sollen. So werden z. B. mit diesem Trick hohe Summen an anonyme Empfänger im Ausland weitergeleitet. Die Betrüger haben diese Summen durch kriminelle Machenschaften oder auch online erbeutet und möchten die Beträge auf dem Umweg über das Konto des „Geldboten“ gerne auf ihren eigenen Konten verbuchen. Dabei bleiben die Täter immer anonym und sind nicht mehr ermittelbar, während sich die Geldboten strafbar machen. In der Regel ermittelt die Staatsanwaltschaft dann nämlich gegen den Geldboten wegen des Verdachts der Geldwäsche, Steuerhinterziehung und evtl. des Internetbetrugs. Erschwerend kommt schließlich noch hinzu, dass die Täter auch über die persönlichen Daten des Opfers inklusive seiner Bankverbindung verfügen und diese ebenfalls missbrauchen können.

Somit ist nachdrücklich vor der Annahme des angeblichen Arbeitsangebotes zu warnen.

Beim Umgang mit unverlangt eingehenden E-Mails ist immer Vorsicht geboten. Das Risiko ist groß, auf unseriöse Werbung hereinzufallen, seinen PC mit Schadprogrammen zu infizieren oder Opfer eines Betrugs oder Identitätsdiebstahls zu werden. Ich empfehle Betroffenen daher stets, solche unverlangten E-Mails kritisch anhand des Absenders und Betreffs zu prüfen und möglichst gar nicht zu öffnen, sondern umgehend zu löschen. Auf keinen Fall sollten die in den E-Mails enthaltenen Links angeklickt, Anhänge geöffnet oder dem Absender geantwortet werden.

Es kann sich dabei aber nicht nur um unseriöse Werbung (sog. „Spam“) oder um Schadprogramme in E-Mail-Anhängen handeln. Oft geht es den Tätern auch darum, wichtige persönliche Daten der E-Mail-Empfänger, wie Zugangsdaten, Bankverbindungen o. Ä., zu erlangen, um diese dann zu Lasten des Betroffenen zu missbrauchen.

4.8
Personalwesen

4.8.1
Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Rechtzeitige Vereinbarungen zur E-Mail- und Internetnutzung am Arbeitsplatz erspart nachträglichen Ärger.

Immer wieder erhalte ich Anfragen, wenn bereits akuter Handlungsbedarf in Bezug auf die Nutzung von E-Mail und anderen Internetdiensten besteht. Sei es, dass der Mitarbeiter, dessen E-Mail-Postfach dringend geöffnet werden muss, nicht erreichbar ist, dass keine Regelung zur privaten Nutzung von E-Mail und Internet getroffen wurde oder dass eine rechtsmissbräuchliche Nutzung von Internetdiensten im Raum steht. Ich rate regelmäßig dazu, eindeutige Regelungen vorab zu treffen, da nachträglich oft kaum noch etwas auszurichten ist.

Hierzu enthält die im Januar 2016 veröffentlichte Orientierungshilfe (https://www.datenschutz.hessen.de/ar009.htm) der Datenschutzaufsichtsbehörden praktische Hinweise und Muster (Ziff. 10.1).

Da die Nutzung von E-Mail und Internet am Arbeitsplatz bislang nicht spezialgesetzlich geregelt ist, kann sich der Leser hier einen Überblick verschaffen, was aus datenschutzrechtlicher Sicht bei der Nutzung dieser Dienste zu beachten ist.

Die Orientierungshilfe wendet sich an private und öffentliche Arbeitgeber, Mitarbeiter, Betriebsräte und an Interessierte. Sie bündelt wiederkehrende Fragen, die an die Aufsichtsbehörden gestellt werden. Im Anhang werden Musterbetriebsvereinbarungen und Einwilligungen vorgestellt, die von Unternehmen und Behörden als Vorlage genutzt werden können.

4.8.2
Öffentlicher Pranger: Personalisierte Krankenstandsliste

Der öffentliche Aushang personalisierter Listen mit den Krankheitstagen einzelner Mitarbeiter ist datenschutzrechtlich unzulässig.

In einem Hotel waren durch den Küchenchef zwei Aushänge mit krankheitsbedingten Fehlzeiten von Küchenmitarbeitern bekannt gemacht worden. Ein Aushang war an der Infotafel des Hotels für alle Mitarbeiter sichtbar angebracht worden, der zweite Aushang befand sich an der Tür neben dem Personaleingang. Unterschrieben waren die Listen mit: „Diese Zahlen muss man sich auf der Zunge zergehen lassen.“
Die Küchenmitarbeiter haben sich an meine Behörde gewandt und darum gebeten, die Angelegenheit datenschutzrechtlich zu überprüfen.

Gesundheitsdaten werden vom BDSG unter einen besonderen Schutz gestellt. Die Verarbeitung dieser besonderen personenbezogenen Daten ist nur unter den engen Voraussetzungen des § 28 Abs. 6 bis 9 BDSG zulässig.

Im konkreten Fall ist § 28 Abs. 6 Nr. 3 BDSG der Maßstab für die Zulässigkeit der Verarbeitung der Krankmeldungen der Beschäftigten. Nach dieser Vorschrift ist die Verarbeitung von besonderen Arten personenbezogener Daten sinngemäß für Geschäftszwecke des Arbeitgebers zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt.

Grundsätzlich ist damit die Speicherung und Verarbeitung von Krankheitstagen nach dieser Vorschrift zulässig, soweit es etwa um Fragen der Fortzahlung des Arbeitsentgelts für Tage, an denen der Beschäftigte aufgrund einer Erkrankung keine Arbeitsleistung erbringen konnte, geht. Das öffentliche Aushängen von krankheitsbedingten Fehlzeiten einzelner Mitarbeiter ist jedoch keinesfalls für den Arbeitgeber erforderlich, um damit seine Ansprüche durchzusetzen, sie ist daher generell unzulässig.

Auch wenn das Arbeitgeberinteresse an einem niedrigen Krankenstand nachvollziehbar ist, rechtfertigt dies nicht die Methode, kranke Mitarbeiter öffentlich anzuprangern.

Dem Geschäftsführer des Hotels habe ich mitgeteilt, dass der Aushang der Liste datenschutzrechtlich unzulässig ist. Er wurde aufgefordert, die Liste unverzüglich zu entfernen und zu vernichten. Dieser Aufforderung wurde sofort nachgekommen.

Das Verhalten des Küchenchefs habe ich beanstandet und den Tatbestand einer Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG festgestellt.

4.8.3
Hinterlegung von Mitarbeiterpasswörtern im Tresor

Im Rahmen einer Beratung wurde mir mitgeteilt, dass die Zugangspasswörter aller Mitarbeiterinnen und Mitarbeiter auf Anweisung der Geschäftsleitung im Tresor aufbewahrt würden. Begründet wurde dies insbesondere mit administrativen Tätigkeiten durch die IT-Betreuung sowie das gelegentlich vorkommende Vergessen eines Zugangspassworts durch Mitarbeiter. Aus Sicht des IT-Betriebes gibt es jedoch keinerlei Gründe für dieses Vorgehen. Vielmehr stehen Belange des Mitarbeiterdatenschutzes dem entgegen. Sofern daher solche Maßnahmen angeordnet sind, sind sie unverzüglich einzustellen.

Gründe aus Sicht des IT-Betriebes, zur Vereinfachung der Tätigkeiten die Zugangspasswörter aller Mitarbeiter in schriftlicher Form – auch verschlossen – gesichert aufzubewahren, gibt es nicht.

- Sofern ein Mitarbeiter sein Passwort vergisst (z. B. nach längerer Abwesenheit oder Urlaub), kann der Administrator über die Benutzerverwaltung einfach und schnell ein neues, temporäres Passwort vergeben. Dieses ist dann durch den Mitarbeiter unverzüglich wieder auf ein nur ihm bekanntes Passwort zu ändern.

- Für administrative Tätigkeiten steht den Administratoren zumindest das bei der Betriebssysteminstallation vorhandene Administratorkonto des Systems zur Verfügung. Aus Gründen der Nachvollziehbarkeit – insbesondere wenn die Administration wechselweise durch mehrere Mitarbeiter erfolgt – sollten hierfür jedoch personalisierte Administratorkonten verwendet werden. Über die als Windows-Standard eingestellte Anzeige des zuletzt erfolgreich angemeldeten Benutzers hat der Mitarbeiter bei der nächsten eigenen Anmeldung dann den Hinweis, welcher Administrator sich an seinem System angemeldet hat (und diesen ggf. nach dem Grund hierfür zu fragen).

- Auch die als weiteren Grund angeführte Anpassung neu installierter Software auf dem System in Abwesenheit des Benutzers stellt keinen hinreichenden Grund für diese Verfahrensweise dar. Aktuelle Software bietet in der heutigen Zeit in der Regel die Möglichkeit, bestimmte, für die interne Nutzung erforderliche oder zweckdienliche Einstellungen vorab zu konfigurieren. Weitergehende oder hierüber nicht mögliche Einstellungen sollten in Absprache und in Anwesenheit des jeweiligen Benutzers erfolgen.
- Außerdem wird durch diese Vorgehensweise der Grundsatz unterlaufen, dass nur dem Benutzer das Passwort zu seinem Konto bekannt ist und somit jedes Handeln mit dem Benutzerkonto ihm auch zuzurechnen ist.

Damit liegt für dieses Vorgehen keinerlei Erfordernis vor und ist daher aus Gründen des Mitarbeiterdatenschutzes und der Datensparsamkeit einzustellen.

4.8.4

Online-Bewerbungen am Beispiel der Software „Interamt“

Die Deutsche Telekom AG (DTAG) bietet vielen hessischen Kommunen, aber auch Unternehmen in Hessen an, mit der Software „Interamt“ ein Recruiting-System bereitzustellen und zu betreiben. Die stellenausschreibenden Auftragnehmer der DTAG wollen im Web präsent sein, um eine möglichst große Zielgruppe zu erreichen. Bewerberinnen und Bewerber sollen sofort auf eine Anzeige elektronisch und online über das Web antworten können. Zudem erscheinen solche Recruiting-Systeme für den Ausschreibenden einer Stelle als attraktiv, weil sie zu versprechen scheinen, dass der gesamte Bewerbungsprozess von Ausschreibung bis Einstellung einer potentiellen Kandidatin oder eines potentiellen Kandidaten auf elektronischem Weg durchgeführt werden kann.

4.8.4.1

Mindestanforderungen an Online-Bewerbungen

Innerhalb eines Web-basierten Verfahrens für Online-Bewerbungen sind nur Daten zu erfassen, deren Kenntnis erforderlich ist, um Eignung, Befähigung und Leistung für den ausgeschriebenen Ausbildungsgang, Dienstposten oder Arbeitsplatz feststellen zu können (§ 11 Abs. 1 HDSG; § 32 BDSG). Die DTAG führt mit ihrem angebotenen Recruiting-System diesbezüglich eine Auftragsdatenverarbeitung durch.

Für die Bewerberinnen und Bewerber muss in den Web-Formularen des Recruiting-Systems, die in der Regel umfangreiche Fragenkataloge darstellen, erkenntlich sein, zu welchem Zweck ihre Daten erfasst werden (§ 13 HDSG). Häufig lassen sich Bewerber/innen verleiten, mehr anzugeben als womöglich erforderlich ist, um ihre Bewerbungschancen zu erhöhen. Hierzu zählen manche Informationen, die als besondere Art von Daten zu kategorisieren sind (§ 7 Abs. 4 HDSG). Beispielsweise gehören dazu Religionsangehörigkeit, Gewerkschafts- sowie Parteizugehörigkeiten oder auch mögliche körperliche Einschränkungen. In diesem Fall ist ein Schutzbedarf von „hoch“ anzunehmen.

Sehr viele persönliche Daten werden an die ausschreibende Stelle übermittelt, bei denen die Bewerberin oder der Bewerber davon ausgehen können muss, dass sie inhaltlich verbindlich sind, in angemessener Zeit verarbeitet werden und ihre Verarbeitung einem nachvollziehbaren Prozess entspricht. Üblicherweise sind Pflichtfelder und freiwillige Eingaben in geeigneter Weise – gut erkennbar für die Bewerberin oder den Bewerber – zu kennzeichnen. In anwendungsspezifischen Datenschutzbestimmungen bzw. in einer konkreten Einwilligung ist über Speicherorte, Speicherfristen und Lösch- und/oder Aufbewahrungsfristen zu informieren (§ 19 HDSG). Bei fehlender Einwilligung ist das Bewerbungsverfahren innerhalb der Web-Applikation abzubrechen (§ 7 HDSG oder § 19a BDSG und § 33 BDSG).

Die Bewerberinnen und Bewerber erwarten, dass ihre Bewerbungsunterlagen nur für das jeweilige Verfahren und das aktuell ausgeschriebene Stellenangebot genutzt werden.

Für das gesamte Bewerbungsverfahren – über die Web-Applikation hinaus – ist sicherzustellen, dass Speicher- und Löschfristen (§ 19 HDSG) gewahrt werden.

Die Bewerberinnen und Bewerber erwarten weiter, dass ihre Bewerbungsunterlagen vertraulich behandelt und ausschließlich an die Personen gegeben werden bzw. jenen zur Verfügung stehen, die gemäß dem jeweiligen Verwaltungsprozess zugrunde liegenden Bewerbungsverfahren adressiert sind (§ 9 HDSG). Die Forderung nach Vertraulichkeit hat somit ihr Pendant sowohl in den personalbezogenen Prozessen der Verwaltung in Kooperation mit dem Personalrat als auch in der Realisierung der Web-Applikation.

Da Initiativbewerbungen, d. h. Bewerbungen, für die es (im Moment) in der Web-Applikation kein passendes Stellenangebot gibt, weiterhin stattfinden, ist auch hier informationstechnisch der Weg eines zweckgebundenen Zugangs – für Initiativbewerbungen (Zugang für Initiativbewerbungen) – vorzusehen. Zunächst wäre es möglich, sich mit einem Hinweis – innerhalb der Web-Applikation für Online-Bewerbungen – zu behelfen, dass Initiativbewerbungen auf dem Postweg zu versenden sind.

4.8.4.2

Zur datenschutzkonformen Nutzung des Recruiting-Systems „Interamt“

Was den Reiz eines Online-Bewerbungsprozesses ausmachen könnte, erweist sich schnell als komplizierte Aufgabe, für die eine komplexe IT-Infrastruktur erforderlich ist. In der Regel können einzelne Kommunen, kleinere oder auch mittelständische Unternehmen kaum selbst dauerhaft betriebsfähig eine entsprechende IT-Infrastruktur vorhalten. Daher sind Web-basierte Online-Bewerbungssysteme sowohl für die DTAG als auch für andere Anbieter ein interessantes und sicherlich auch profitables Geschäftsfeld.

Für diesen Zweck sind Verträge über eine Datenverarbeitung im Auftrag (ADV) erforderlich. Bei Stellen, die dem HDSG unterfallen, hat mich der Auftraggeber vorab über die Beauftragung nach § 4 Abs. 3 HDSG zu unterrichten. Diese Software wird in verschiedenen hessischen Kommunen bereits eingesetzt. Leider wurde ich von einigen hessischen Kommunen nicht über eine ADV mit der Software „Interamt“ unterrichtet.

4.8.4.3

Prüfungen des Recruiting-Systems „Interamt“ seit 2015

Bereits am 26.05.2015 habe ich bei einer hessischen Kommune vor Ort über Vorbehalte aus juristischer und informationstechnischer Sicht bzgl. des Recruiting-Systems „Interamt“ mit der DTAG gesprochen. Die juristischen Probleme im ADV-Vertrag wurden daraufhin schnell ausgeräumt.

Außerdem waren sich die Vertreter der bei der Prüfung beteiligten Stellen (Kommune, DTAG und HDSB) einig, dass die Software „Interamt“ auch besondere Arten von personenbezogenen Daten (nach § 3 Abs. 9 BDSG respektive § 7 Abs. 4 HDSG) verarbeitet. Jedoch wurde dies bei der Realisierung nicht berücksichtigt, da es sich nach Angaben des DTAG-Vertreters um ein historisch gewachsenes System handelt, welches schon lange existiert und zu Beginn nur wenige Funktionen hatte.

Wenn eine hessische Kommune bei der DTAG die Nutzung des Recruiting-Systems „Interamt“ einkauft, dann werden die Daten der Bewerberinnen und Bewerber bei der DTAG gemäß der ADV gespeichert. Bewerberinnen und Bewerber vertrauen bei ihrer Bewerbung jeweils der datenschutzkonformen Verarbeitung durch die jeweilige Kommune. Die Kommune, vertreten durch die Personalabteilung der Kommune, wird zum Mandanten während der Nutzung des Recruiting-Systems „Interamt“. Wenn die Trennung der Speicherorte für die einzelnen Kommunen nicht ausreichend umgesetzt ist, besteht die Möglichkeit, dass unbefugte Dritte, wie eine andere Kommune, auf die Bewerbungen zugreifen können. Nur mit einer entsprechenden Trennung der Mandanten – hier der Daten der jeweiligen Kommunen – bis auf die Ebene der Speicherorte ist eine datenschutzkonforme Verarbeitung gewährleistet.

Als Ergebnis der Prüfung vom 26.05.2015 sollten in die Release-Planung der Software „Interamt“ insbesondere folgende Anforderungen aufgenommen werden, um den Anforderungen an einen höheren Schutzbedarf gerecht zu werden:

- die Möglichkeit der 2-Faktor-Authentisierung (2FA) und
- eine weitere logische Trennung bzgl. der Mandanten.

Die Umsetzung dieser Anforderungen wurden mir von DTAG-Vertreterinnen und –Vertretern zugesagt.

Seit Frühjahr 2016 gab es erneut mehrere und fortlaufende Anfragen von hessischen Kommunen bzgl. einer Nutzung des Recruiting-Systems „Interamt“. Seit 10.02.2016 bin ich mit der DTAG in regelmäßigem Kontakt. Dabei habe ich festgestellt, dass bisher lediglich eine Möglichkeit der 2FA geschaffen wurde, die dennoch weiterhin besonders zu konfigurieren ist. Wünschenswert ist, dass die 2FA selbstverständlich würde, um einen heute üblichen technischen Mindeststandard aus dem Bereich der IT-Sicherheit bei der Verarbeitung von besonderen Arten personenbezogener Daten zu wahren.

4.8.4.4

Weiterhin bestehende nicht datenschutzkonforme Verarbeitung im Recruiting-System „Interamt“

Weiterhin ist kritisch in Bezug auf die Nutzung des Recruiting-Systems „Interamt“ der DTAG zu betrachten:

1. Die DTAG setzt ein teilautomatisiertes PSA-Verfahren (Privacy and Security Assessment) ein, das bei einer entsprechenden Kategorisierung von personenbezogenen Daten nach dem Schutzbedarf – also auch für besondere Arten von personenbezogenen Daten – die Zuständigen anleitet bzw. unternehmensintern vorschreibt, welche technischen und organisatorischen Maßnahmen (TOMs) für die datenschutzkonforme Verarbeitung der personenbezogenen Daten zu ergreifen sind.

   Gemäß eigener Auskunft der DTAG soll dieses Verfahren zur Kategorisierung vom Vorgänger der Bundesbeauftragten für den Datenschutz und die Informationssicherheit beurteilt und als ordnungsgemäß angesehen worden sein.

2. In der tatsächlichen Anwendung des genannten Verfahrens zur Kategorisierung der personenbezogenen Daten gibt es sehr unterschiedliche Auffassungen. Die DTAG erklärt, dass nach einer im August 2016 erwirkten höheren Kategorisierung der zu verarbeitenden personenbezogenen Daten in „Kategorie Datenschutz A“ (höchste Kategorie) aus Sicht der DTAG keine zusätzlichen technischen und organisatorischen Maßnahmen (TOM) i. S. d. Anlage zu § 9 BDSG erforderlich sind. Mit der Kategorisierung in „A“ ist die Begleitung des Verfahrens durch den Bereich Datenschutz der DTAG verbunden. Ein Verfahren wird im Gesamten durch diesen Bereich Datenschutz bewertet und einzelne Entscheidungen zur Umsetzung von datenschutzrechtlichen Anforderungen werden gemäß dem genannten PSA-Verfahren dokumentiert.

3. Die von der DTAG beschriebene und angedachte Lösung für eine weitere logische Trennung der Mandanten für die Software „Interamt“ bleibt unzureichend: Durch eine Behörden-Tabelle, die die so genannten Behörden-IDs enthält und mit den „Interamt“-Tabellen verknüpft ist, wird eine Einschränkung über Behörden-Ids in den SQL-Anfragen auf Anwendungsebene ermöglicht. Dies bewirkt, dass der Anwenderin oder dem Anwender nur Daten ihrer oder seiner Behörde angezeigt werden, wenn das System fehlerfrei arbeitet.

   Zu fordern ist, dass mindestens ein weiterer Trennungsmechanismus eingeführt wird. Der zusätzliche, unabhängige Mechanismus muss gewährleisten, dass bei Versagen der ausschließlich über die Behörden-ID gesteuerten Implementierung weiterhin bspw. Behörde A keine Daten einer Behörde B zur Kenntnis nehmen oder gar verändern kann. Die von der DTAG beschriebene Lösung gewährleistet dies aber nicht, da sie ebenfalls auf Anwendungsebene angesiedelt ist und für die schon existierende erste Trennung mittels Rechte- und Rollenkonzepts benötigt wird; also keine weitere Trennung darstellt.

4. In den Anforderungen des genannten PSA-Verfahrens der DTAG sind als TOMs für eine getrennte Verarbeitung auch die folgenden Punkte genannt:
   - unterschiedliche physische/logische Komponenten (z. B. unterschiedliche physische oder virtuelle Server)
   - getrennte Tabellen, Verzeichnisse oder Dateien

Meine Vorbehalte begründen sich
- aus einer Kategorisierung der zu verarbeitenden personenbezogenen Daten mittels des von der DTAG eingesetzten „Privacy & Security Assessments“, da die von mir erwirkte höhere Kategorisierung in „Datenschutz A“ noch nicht zwingend bedeuten muss, dass weitere technische, notwendige und geeignete Maßnahmen ergriffen werden, die auch dauerhaft im Betrieb zur Verfügung stehen,
- folglich einer unzulänglichen Umsetzung der TOMs bzgl. der eigenen Anforderungen, die sich aus der Anwendung des PSA-Verfahrens ergeben sollten, und
- einer weiteren logischen Trennung von Mandanten.

Da meine informationstechnischen Vorbehalte bisher nicht ausgeräumt werden konnten, habe ich die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen in Kenntnis gesetzt, da die DTAG ihren Unternehmenssitz in Nordrhein-Westfalen hat und deshalb in deren Zuständigkeitsbereich liegt.

Zudem habe ich am 15.09.2016 in einer Presseerklärung ausgeführt, dass die Nutzung des Recruiting-Systems „Interamt“ nur unter den folgenden Auflagen rechtlich zulässig ist:
- Die Stellenausschreibungen im Web über das Portal „Interamt“ müssen einen augenfälligen Hinweis mit der Erklärung enthalten, dass eine datenschutzkonforme Verarbeitung nicht in allen Fällen gewahrt ist; denn die bestehende Software „Interamt“ garantiert nicht, dass besondere Arten personenbezogener Daten nach § 7 Abs. 4 HDSG bzw. § 3 Abs. 9 BDSG in Bewerbungen ordnungsgemäß verarbeitet werden.
- Mindestens solange dieser Mangel nicht behoben ist, muss für Bewerberinnen und Bewerber der Postweg erhalten bleiben, um eine datenschutzkonforme Übersendung der Bewerbungen zu ermöglichen. Die auf dem Postweg erhaltenen Bewerbungen dürfen nicht in der Software „Interamt“ nacherfasst werden.

Bei der Auswahl und Umsetzung solcher Online-Bewerbungsverfahren ist dies zwingend zu berücksichtigen.

Am 29.11.2016 suchte mich der Datenschutzbeauftragte der DTAG in Begleitung von Personen aus der Technik und dem Vertrieb auf. Während dieses Gesprächs sind wir übereingekommen, dass in Hinblick auf die technischen Maßnahmen eine bessere Lösung zu finden sei. Die DTAG brachte eine entsprechende Idee mit, zu deren Ausführung weitere Belege nachzureichen sind, so dass eine Bewertung möglich wird. Dabei ist zu berücksichtigen, inwiefern auch im dauerhaften Betrieb damit die Interessen der Bewerberinnen und Bewerber in Bezug auf die datenschutzrechtlichen Anforderungen gewahrt bleiben. Die technische Bewertung wird selbstverständlich in enger Kooperation mit der Landesdatenschutzbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen erfolgen.

5. Technik und Videoüberwachung

5.1

Entwicklungen und Empfehlungen im Bereich der Informationstechnik

5.1.1

Verschlüsselter Nachrichtenaustausch: Wann ist ein Encryption-Gateway eine Alternative?

Um eine vertrauliche und integre Kommunikation zu gewährleisten, gibt es mehrere technische Lösungen. Doch jede Umsetzung muss mit Bezug auf die technischen und organisatorischen Maßnahmen den datenschutzrechtlichen Gewährleistungszielen der Vertraulichkeit und der Integrität genügen. Schließlich bedingen die Fragen nach der Häufigkeit der Kontaktaufnahme und die Gruppe der möglichen Adressierten die Auswahl der einzusetzenden Methoden. In der folgenden Darstellung ist ein datenschutzkonformer Nachrichtenaustausch, z. B. per E-Mail, mit Realisierungen von Transport- und Datensicherheit im Fokus.

Da ich mehrere Eingaben und Anfragen erhalten habe, in denen eine sichere Kommunikation und deren Mittel zu prüfen waren, möchte ich das Thema der vertraulichen und integren Kommunikation erneut aufgreifen. Das Bedürfnis ist deutlich gestiegen, sich gegen unbefugte Zugriffe zu schützen. Nutzende wie Betreibende hatten besonders Fragen zu so genannten Encryption-Gateways und das auch im Vergleich zu anderen Anwendungsszenarien basierend auf einer *Public Key Infrastructure* (PKI).

5.1.1.1

Zu realisierende Gewährleistungsziele

Das Gewährleistungsziel Vertraulichkeit ist mit der Anforderung verbunden, Daten vor unbefugter Preisgabe zu schützen. Mit der Forderung nach Integrität ist verbunden, dass die Daten vollständig und unverändert sind. Aus der technischen Perspektive sind Transport- und Datensicherheit Voraussetzungen, um eine vertrauliche und integre, elektronische Kommunikation zu gewährleisten. Die dazugehörige Transportverschlüsselung zielt auf die Sicherung der Verbindung bzw. des Übertragungskanals. Die übertragenen Daten selbst müssen hierbei nicht verschlüsselt sein. In Netzen gehört dazu die Anwendung der Protokolle, die ein „s“ für „secure“ enthalten, wie *https*, *sftp*, *scp* u.v.m.

Die Datensicherheit zielt bei einer elektronischen Kommunikation auf die Verschlüsselung von Daten, d. h., die zu übertragende Datei bzw. der Inhalt z. B. einer Mail ist verschlüsselt, bevor sie übertragen wird. Das ist eine Verschlüsselung auf der Applikationsebene, für die innerhalb der Anwendung entsprechende Verschlüsselungsverfahren eingebunden sein müssen. Dabei kann der Übertragungsweg ggf. ungesichert bleiben.

Wenn für die elektronische Kommunikation sowohl Transport- als auch Datensicherheit realisiert sind, wird von einer Ende-zu-Ende-Verschlüsselung gesprochen – so gemäß der formalen, wissenschaftlichen Definition.

In der Praxis wird bereits oft von einer Ende-zu-Ende-Verschlüsselung gesprochen, wenn zwischen Sender – dem Rechner, von dem die Nachricht versandt wird – und Empfänger – dem Rechner, bei dem die Nachricht ankommt und bei dem E-Mail-Adresse als Zieladresse verwaltet wird – eine durchgängige verschlüsselte Übertragung erfolgt.

Die Grenzen der Nutzung von Ende-zu-Ende-Verschlüsselungen liegen in ihrer praktischen Verwendung. So beklagen immer noch viele Nutzende, dass die eingesetzte Technologie zu schwierig sei, um sie täglich zu verwenden. Bei der geäußerten Kritik ist leider auch immer wieder festzustellen, dass Herangehensweisen miteinander verglichen werden, die sich in ihrer technischen Umsetzung unterscheiden. Im Folgenden möchte ich darlegen, wann welche Methode mit dem größten Gewinn aus datenschutzrechtlicher Sicht einzusetzen ist.

5.1.1.2
Häufigkeit der Kontaktaufnahme und öffentliche Schlüssel

Die Frage nach der Häufigkeit der Kontaktaufnahme zum Nachrichtenaustausch – oftmals über E-Mail – bestimmt auch die Auswahl der einzusetzenden Methoden. Zu unterscheiden sind,

- ob es sich um eine einmalige oder sich selten wiederholende Kontaktaufnahme zwischen zwei oder auch mehreren Kommunikationspartnerinnen und -partnern handelt,
- ob ein stetiger Austausch von Nachrichten ggf. mit wechselnden Sendern zu einer zentralen Stelle zu erwarten ist oder
- ob es fortwährend die zwei gleichen Kommunikationspartnerinnen und -partner sind, die häufig Nachrichten per E-Mail austauschen.

Public Key-Infrastrukturen (PKI) dienen der Einbindung von vielfältigsten Anwendungen in eine einheitliche Sicherheitsumgebung, die Verschlüsselungsmechanismen in Netzen bereitstellen. Heute sind einer PKI verschiedene kryptografische Verfahren inhärent, mit denen auf elektronischem Weg die Sicherheitsfunktionen in Netzen bereitgestellt werden: Vertraulichkeit durch Verschlüsselungsverfahren, Datenintegrität durch z. B. Hash-Funktionen oder auch Authentizität durch eine digitale Signatur. Eine PKI ist vielseitiger einsetzbar als am Beispiel des sicheren Nachrichtenaustauschs per E-Mail dargestellt werden kann; doch ist der „sichtbare“ Nachrichtenaustausch der häufigste Anlass zu Nachfragen bei mir.

Da der sichere Austausch des gemeinsam zu nutzenden, geheimen Schlüssels bei symmetrischen Verschlüsselungsverfahren problematisch sein kann, wird im Weiteren die Nutzung einer asymmetrischen Verschlüsselung innerhalb einer PKI betrachtet.

Um die unterschiedlichen, realisierten Abläufe darzustellen, ist zwischen bereits Teilnehmenden an der Nutzung einer PKI und potentiellen Kommunikationspartnerinnen und Kommunikationspartnern, für die ein verschlüsselter Nachrichtenaustausch angestrebt ist, zu unterscheiden. Für Teilnehmende gibt es bereits ein valides Schlüsselpaar, das innerhalb der PKI verwaltet wird. Eine asymmetrische Verschlüsselung verlangt die Nutzung eines Schlüsselpaares, das der jeweiligen Teilnehmerin bzw. dem jeweiligen Teilnehmer zugeordnet ist. Das Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. Der private Schlüssel verbleibt als individueller und geheimzuhaltender Schlüssel bei der Teilnehmerin bzw. dem Teilnehmer. Der öffentliche Schlüssel muss jeweils der anderen Kommunikationspartnerin bzw. dem anderen Kommunikationspartner zur Verfügung gestellt werden.

Im Allgemeinen ist jetzt die zu versendende Datei mit dem öffentlichen Schlüssel der Empfängerin oder des Empfängers zu verschlüsseln, so dass nur die adressierte Person mit Hilfe des dazu passenden privaten Schlüssels die Nachricht entschlüsseln und damit lesen kann. Ein weiterer Vorteil der asymmetrischen Verschlüsselung ist, dass die Infrastruktur auch geeignet ist, digitale Signaturen zu unterstützen. Der öffentliche Schlüssel kann in verschiedener Weise in Anwendungen integriert werden. Die Art und Weise, wie die entsprechenden öffentlichen Schlüssel verwendet werden, bestimmt auch die

Systemarchitektur der einsetzenden Methoden: in E-Mail-Systemen, über Portal-Lösungen oder auch über so genannte Encryption-Gateways.

5.1.1.3

In E-Mail-Systemen: Häufige Kontaktaufnahme zwischen zwei Instanzen

Wenn zwei Kommunikationspartner häufig E-Mails miteinander austauschen, ist die Wahl einer asymmetrischen Verschlüsselung mit zu nutzender PKI empfehlenswert. Dazu haben die Personen ihre öffentlichen Schlüssel auszutauschen, die zudem zertifiziert sein sollten. Dringend ist ein Schlüsselpaar mit einer Gültigkeitsdauer zu versehen, damit spätestens nach deren Ablauf eine neue Prüfung stattfindet, ob Sender und Empfänger die vertrauten Personen sind.

Ein öffentlicher Schlüssel kann in einer unverschlüsselten E-Mail an die spätere Senderin bzw. den späteren Sender vorab versandt werden. Im Weiteren kann dann die Senderin oder der Sender die E-Mails an den Empfänger mit dessen öffentlichen Schlüssel immer verschlüsseln. Öffentliche Schlüssel lassen sich auch auf einer Web-Seite im Netz publizieren, auf der die Person sie findet, die Kontakt aufnehmen möchte.

Wenn ein zertifizierter, öffentlicher Schlüssel verwendet wird, dann kommt ein so genanntes Trustcenter ins Spiel. Ein Trustcenter ist eine Zertifizierungsstelle, die digitale Zertifikate für „beglaubigte“ Schlüssel vorhält. Die Beglaubigung der Schlüssel geschieht, indem die Teilnehmende oder der Teilnehmende nachweist, die Person zu sein, die sie oder er vorgibt zu sein. Dabei legt das Trustcenter fest, wie die Authentizität geprüft wird, z. B. durch persönliches Vorbeikommen, Vorlage eines amtlichen Dokuments oder Ausweises. Bei einem erfolgreichen Nachweis wird mit einem solchen Zertifikat durch das Trustcenter der Zusammenhang zwischen einer natürlichen Person und dem ihr zugeordneten öffentlichen Schlüssel bescheinigt; d. h., es betreibt ein Verzeichnis, gegenüber dem potentielle Kommunikationspartner automatisch prüfen können, ob ein Zertifikat gültig ist. Das gültige und automatisch prüfbare Zertifikat ersetzt somit eine Authentizitätsprüfung vor Ort, da diese vorher durch das Trustcenter stattfand. Des Weiteren betreibt ein ordentliches Trustcenter auch noch eine Sperrliste ungültig gewordener Schlüssel bzw. der dazugehörigen Zertifikate, die es beglaubigte und bei denen die automatisierte Echtheitsprüfung jetzt fehlschlägt.

Im persönlichen und privaten Umfeld wird anstatt des Trustcenters gerne eine „Kette“ von gegenseitigem Zuspruch von Vertraulichkeit und Authentizität gebildet. Jemand bestätigt jemanden, dass er sie oder ihn kennt und sie oder er bestätigt es einer weiteren Person. Um dieses Vorgehen zu beschleunigen und die entsprechenden Zertifikate per Wechselmedien auszutauschen, werden so genannte Crypto-Partys veranstaltet.

Des Weiteren empfiehlt es sich dann langfristig bzw. für die Gültigkeitsdauer der Schlüssel, zertifizierte, öffentliche Schlüssel auszutauschen und in einem Schlüsselspeicher ergänzend in der eigenen Mail-Applikation entsprechend für jede Kommunikationspartnerin oder jeden Kommunikationspartner zu hinterlegen. Für die meisten E-Mail-Systeme ist ein entsprechendes Plugin verfügbar und einfach zu installieren. Nach der Installation des Plugins kann der Sendende bei jedem Versand einer E-Mail für den adressierten Empfänger entscheiden, ob die E-Mail zu verschlüsseln, mit einer digitalen Signatur oder mit beidem zu versehen ist. Heute reichen in den Applikationen zumeist ein bzw. zwei Klicks, um zu verschlüsseln oder die E-Mail mit einer digitalen Signatur zu versehen. Dabei werden die Dateiinhalte bzw. die Nachricht verschlüsselt. Ob zusätzlich die Datenübertragung im Netz verschlüsselt ist, hängt vom Ausbau des Netzes ab. Hierfür kann in diesem Fall keine generelle Aussage getroffen werden, obwohl zunehmend davon auszugehen ist, dass auch zwischen den Routern und Switchen gesicherte Protokolle eingesetzt werden.

In Abhängigkeit der Funktionalität und der Konfiguration gibt es inzwischen einige Plugins, bei denen die im eigenen Schlüsselspeicher vorliegenden öffentlichen Schlüssel auf ihre Gültigkeit und ihre Echtheit vor dem Versand einer verschlüsselten E-Mail geprüft werden, ohne dass der Nutzende jedes Mal die Abfrage gegenüber dem im Trustcenter hinterlegten Zertifikat starten muss.

Diese Lösung zur Umsetzung einer integren, vertraulichen Kommunikation, bei der die Daten bzw. Nachrichteninhalte verschlüsselt werden, ist mit Aufwand für den Nutzenden in der Einstiegsphase verbunden. In dieser Phase

- muss sie oder er sich gegenüber dem Trustcenter authentifizieren oder innerhalb einer Crypto-Party einem vertrauensvollen Kreis anschließen,
- den öffentlichen Schlüssel mit der jeweiligen direkten Kommunikationspartnerin oder mit dem jeweiligen Kommunikationspartner austauschen und
- ggf. ein passendes Plugin in das E-Mail-System bzw. in den eigenen E-Mail-Client integrieren.

Danach ist das Versenden und Empfangen in gewohnter Weise möglich.

Dieses Vorgehen unter Nutzung eines Trustcenters oder dem Besuch einer Crypto-Party fällt unter die Kategorie des „Selbstdatenschutzes“. Jede oder jeder kann aktiv werden. Auf einer Crypto-Party finden Neulinge oftmals auch technische Unterstützung, diese genannten Schritte für den eigenen E-Mail-Client auszuführen.

5.1.1.4
Über Portal-Lösung:
Regelmäßige Kontaktaufnahme zu einer zentralen Stelle

Wenn eine regelmäßige Kontaktaufnahme zu einer zentralen Stelle zu erwarten ist, dann empfiehlt sich eine Portal-Lösung. Eine solche Portal-Lösung nennt eine E-Mail-Adresse, an die gesendet wird, und bietet einen öffentlichen Schlüssel. Portal-Lösungen verlangen, dass der öffentliche Schlüssel frei zugänglich ist. In der Regel ist der öffentliche Schlüssel auf der Web-Seite der zentralen Stelle bereitgestellt, so dass er leicht zu finden ist und direkt genutzt werden kann. Um die Portal-Lösung bzw. den Server mit der entsprechend zur Verfügung gestellten Web-Seite möglichst wenig angreifbar zu machen, ist zu empfehlen, die Anzeige bzw. den Zugriff auf die Seite über ein *https*-Protokoll abzusichern. Hier ist der Publikationsweg des öffentlichen Schlüssels bzw. der Übertragungskanal beim entsprechenden Download ebenfalls entsprechend zu schützen.

Die Verschlüsselung des E-Mail-Verkehrs kann jetzt auf unterschiedliche Weise durchgeführt werden. In der ersten Variante importiert sich die Senderin oder der Sender den öffentlichen Schlüssel in den Schlüsselmanager des eigenen E-Mail-Client, falls ein Plugin – wie oben beschrieben – integriert ist. Anschließend kann eine E-Mail geschrieben, verschlüsselt und verschickt werden. Eine zweite Variante ist für Nutzende in der Bedienung zunächst etwas komfortabler. Innerhalb des Portals wird ein Formular integriert, in das die Senderin oder der Sender ihre oder seine Nachricht schreibt. Beim Klicken auf einen Senden-Button innerhalb der Web-Oberfläche wird die Nachricht automatisch verschlüsselt. Wenn diese Implementierungsstrategie gewählt ist, ist gleichzeitig darauf zu achten, dass die Zeicheneingabe und die Übertragung aus dem Formular in der Web-Oberfläche transportgesichert sind; d. h. die übertragenden Daten durch keinen Dritten mitgelesen werden. Wie ausgeführt, empfehle ich sowohl die Verschlüsselung der Daten als auch die Sicherung des Übertragungskanals.

Teilweise wird behauptet, dass eine Absicherung des Übertragungsweges innerhalb der Web-Applikation mittels des Protokolls *https* genügen würde, weil die Applikation in der eigenen Umgebung läuft, die von der IT-Abteilung kontrolliert wird. Diese Einschätzung halte ich für zu kurz gegriffen und teile sie nicht. Denn die Implementierungen als Web-Applikation können auf verschiedenen Versionen von Protokollen basieren, die abwärts kompatibel sein müssen. Diese Form der Kompatibilität ist erforderlich, damit der Nachrichtenaustausch im gesamten Netz möglich bleibt. Aber es bestehen z. B. gravierende Unterschiede zwischen den Protokoll-Versionen von TLS 1.0 (bzw. SSL 3.0) und der späteren Version TLS 1.2. Für den Nutzenden ist nicht unbedingt zu erkennen, welche Version der Protokolle der Web-Applikation unterliegt, insbesondere dann nicht, wenn mehrere Weiterleitungen im Netz stattfinden.

Für die beiden genannten Fälle einer ersten Kontaktaufnahme über eine Portal-Lösung gilt: Wenn die Senderin oder der Sender als Antwort vom Empfänger eine ebensolche verschlüsselte E-Mail erhalten möchten, dann muss sie oder er dem Empfänger ihren bzw. seinen öffentlichen Schlüssel zukommen lassen. Anschließend verläuft die weitere verschlüsselte Kommunikation, wie bereits für die Kommunikation zwischen zwei Instanzen beschrieben.

Eine solche Portal-Lösung kann auch von klein- und mittelständischen Betrieben über einen eigenen, dauerhaft zur Verfügung gestellten Server mit unterlegtem zertifiziertem Schlüsselpaar – angebunden an eine E-Mail-Adresse *poststelle@unternehmensname.com* – betrieben werden. Inzwischen gibt es mehrere Lösungen *out-of-the-box*, die mit einem überschaubaren Aufwand zu konfigurieren sind, so dass mit fallender Tendenz Gesamtkosten im Jahr von ungefähr 1.000 EUR anfallen. In der Kalkulation für das Jahr 2016 sind Arbeitskosten, ein entsprechender einfacher Server mit Hard- und Software und Kosten für die Zertifizierung des Schlüsselpaars einkalkuliert.

Eine solche Portal-Lösung mit sicherer Übertragung und verschlüsselten Daten der Nachricht vereinfacht den Erstkontakt und senkt die Hemmschwelle deutlich für diejenigen, die Vertraulichkeit erwarten.

5.1.1.5
Encryption-Gateway:
Einmalige oder seltene Kontaktaufnahme

Für eine einmalige oder sich selten wiederholende Kontaktaufnahme zwischen zwei oder auch mehreren Kommunikationspartnerinnen und -partnern kann ein Encryption-Gateway die geeignete Lösung sein. Das Encryption-Gateway dient dem Austausch von Nachrichten, die innerhalb des Gateways in verschlüsselter Form vorliegen und auf die über ein Web-basiertes Interface zugegriffen wird. Zumeist wird das Encryption-Gateway von einem größeren Unternehmen mit IT-Abteilung angeboten und betrieben, die eine Web-basierte Portal-Lösung für ihre Online-Dienste bereitstellt, so dass ein integraler Bestandteil bereits eine PKI ist.

Der Zugriff auf das Web-basierte Interface innerhalb einer Portal-Lösung hat über ein sicheres Protokoll, z. B. *https,* zu erfolgen. Die Authentizität der Nachrichtenempfängerin oder des Nachrichtenempfängers wird über ein spezielles Login geprüft. Dazu ist vorab eine Benutzerkennung zu hinterlegen. Diese Benutzerkennung beinhaltet oftmals eine E-Mail-Adresse derjenigen oder desjenigen, die oder der die Nachricht erhalten soll.

Der Nachrichtenaustausch funktioniert dann in folgender Weise:

1. Die Empfängerin oder der Empfänger, die oder der durch das Unternehmen angeschrieben wird, erhält an die hinterlegte Mail-Adresse eine so genannte Notifikation, dass eine Nachricht für sie oder ihn vorliegt.
2. Die Notifikation ist eine E-Mail-Nachricht – selbst unverschlüsselt –,die zumeist einen automatisch erzeugten Link enthält, der den verschlüsselten und personalisierten Zugriff auf die im Web-Portal vorliegende Nachricht gestattet.
3. Der Link ist eine zusammengesetzte URL und beinhaltet
    a. zumeist die Web-Adresse für das Web-Portal,
    b. die schon erwähnte E-Mail-Adresse und
    c. eine eindeutige Zuordnung.
4. Der Link ist aus der E-Mail mit der Notifikation klickbar (oder er kann in ein geöffnetes Browser-Fenster kopiert werden).
5. Mit der Evaluierung der URL erfolgt ein Redirect in das Web-Portal des Unternehmens, bei deren Anmeldung das Einmalpasswort geprüft wird und der Empfänger vor die Auswahl gestellt wird, ob weitere Nachrichten zu erwarten sind (oder nicht).
    a. Wenn eine umfassendere Kommunikation beginnt, dann kann die Empfängerin oder der Empfänger ein eigenes Passwort setzen, mit dem sie oder er sich zukünftig einloggt. Dabei ist entsprechenden Nutzungsbedingungen oder auch AGBs zuzustimmen.
    b. Wenn sie oder er sich für eine einmalige Anmeldung entscheidet, dann gelten in der Regel strengere Nutzungsbedingungen, denen auch zuzustimmen ist.
6. Wenn den Bedingungen zugestimmt wurde, dann erfolgt der tatsächliche Zugriff auf die Nachricht, die die Empfängerin oder der Empfänger erhalten soll.
7. Innerhalb dieses Zugriffs kann sie oder er zumeist gleich auf die Nachricht innerhalb des Web-Portals des Unternehmens antworten.
8. Die sendende Stelle oder Person wird zum Empfänger; es können auch mehrere Empfänger sein, die die Antwort erhalten.
9. Die Nachricht muss – meist durch Klick auf einen Sende-Button – verschickt werden.
10. Die Empfänger erhalten ebenso eine Notifikation und der Prozess des Nachrichtenaustauschs beginnt von vorn.

Bei dieser Systemarchitektur für ein Encryption-Gateway mittels des erläuterten Web-basierten Zugriffs obliegt die Verschlüsselung allein dem Betreiber des Portals, wobei wieder sowohl Übertragungskanal als auch die tatsächliche Nachricht zu verschlüsseln sind. Zu beachten ist, dass unter Verwendung des Encryption-Gateways in der Regel die Kontaktaufnahme durch den Betreiber initiiert wird. Dazu muss ihm die E-Mail-Adresse des Empfängers bekannt sein. Die E-Mail-Adresse wird zumeist auf einem anderen Kommunikationsweg erfragt. Die Verwaltung von E-Mail-Adressen ist beim Encryption-Gateway nicht mehr zwingend dem System inhärent, wie es bei den anderen Formen der verschlüsselten Kommunikation vorauszusetzen ist, wenn eine wechselseitige Kommunikation fortgesetzt wird. Insgesamt gelten bzgl. der einzusetzenden Verschlüsselungen für das Encryption-Gateway die gleichen technischen und organisatorischen Maßnahmen wie für die Web-basierte Portal-Lösung, bei der die Kundin oder der Kunde den Erstkontakt herstellt. Anzumerken bleibt, dass, falls der Link für den Zugriff über das Web-Portal in den Besitz von unbefugten Dritten gelangt, die Nachricht im Portal des Unternehmens auch nicht mehr geschützt ist. Daher kann diese Form der Kommunikation nur als sicher angesehen werden, wenn der Versand der Notifikation per E-Mail transportverschlüsselt erfolgt. Die Nachrichten verbleiben im Bereich des Unternehmens, außer eine Download-Funktionalität wird vorgesehen. Bei den Nutzungsbedingungen ist also genau zu beschreiben, ab wann die Eigenverantwortung des Nutzenden beginnt. Ein heruntergeladenes Dokument kann, muss aber nicht mehr verschlüsselt sein. Wenn es nicht mehr verschlüsselt ist, muss die nutzende Person, bspw. die Kundin oder der Kunde des Unternehmens, explizit darauf hingewiesen werden, dass die Gewährleistungsziele Vertraulichkeit und Integrität vom Unternehmen nicht mehr gewährleistet werden können. Ein Beispiel für diese Verletzlichkeit ist, wenn sich das heruntergeladene Dokument an einem Speicherort befindet, auf den noch andere Personen Zugriff haben.

Diese Form der Kommunikation ist tatsächlich nur für die sporadische Kontaktaufnahme geeignet, bei der keine sensiblen Daten ausgetauscht werden.

5.1.1.6
Digitale Signatur

Ein weiterer Sicherungsmechanismus ist die digitale Signatur. Eine digitale Signatur bestätigt die Integrität der gesendeten Daten und die Authentizität des Senders gegenüber den Empfangenden. Deshalb wird bei einer Signatur auch oft von einer digitalen Unterschrift gesprochen.

Mit einer digitalen Signatur können nicht nur einzelne Dokumente bzw. deren enthaltene Daten versehen werden, sondern auch gesamte technische Prozesse, die in automatisierter Weise die Herkunft von Nachrichten bzw. deren unbestreitbare Urheberschaft z. B. aus einem Unternehmen bestätigen. Die digitale Signatur ist ein zusätzliches digitales Mittel, das neben der Verschlüsselung steht. Es müssen weder die Daten verschlüsselt noch der Übertragungskanal gesichert sein. Aber wenn Vertraulichkeit und Integrität vollständig gewährleistet sein sollen, dann kann nicht von der Verschlüsselung abgesehen werden.

Eine Signatur mit einem zertifizierten Schlüssel und zertifizierten Komponenten ist höher einzuschätzen als mit einem selbst erstellten Schlüssel. Das Verfahren zur Zertifizierung eines Signaturschlüssels findet ebenfalls über ein Trustcenter statt und funktioniert in der Grundfunktionalität in gleicher Weise wie für einen zertifizierten Verschlüsselungsschlüssel. Des Weiteren wird die Güte einer Signatur unterschieden: fortgeschrittene und qualifizierte Signaturen (fortgeschrittene elektronische Signaturen gemäß § 2 Nr. 2 Signaturgesetz (SigG) bzw. qualifizierte elektronische Signaturen gemäß § 2 Nr. 3 SigG).

In jede der genannten Implementierungen kann eine digitale Signatur integriert werden.

5.1.1.7
Grenzen der Verschlüsselung in Netzen

Um eine Ende-zu-Ende-Verschlüsselung vollständig umzusetzen, ist zu diskutieren,

- welche technischen Gegebenheiten beim Versand zu berücksichtigen sind bzw. welche Netzknoten auf dem Weg durch die Netze mit Nachrichten passiert werden, und
- welche Empfängerinnen und Empfänger oder auch Systeme als ein „Ende“ aufzufassen sind.

Für eine umfassende Ende-zu-Ende-Verschlüsselung sind nach Begriffsdefinition sowohl eine Transport- als auch eine Inhaltsverschlüsselung gefordert. Auf dem Transportweg kann es dazu kommen, dass für den korrekten Weitertransport zwischen unterschiedlichen Netzen die Transportverschlüsselung zu brechen ist und erneut verschlüsselt werden muss. Dieses Ent- und Verschlüsseln geschieht bei ordnungsgemäß installierten und konfigurierten Netzen vollautomatisch. Im Fehlerfall kann es sein, dass die Transportverschlüsselung aufgebrochen ist und der Übertragungsweg unverschlüsselt bleibt. Das ist eine echte Schwachstelle der Transportverschlüsselung. Daher werde ich immer die sichere Variante, nämlich die Verschlüsselung der eigentlichen Daten bzw. des Inhalts einer Nachricht, vorziehen, wenn zwischen beiden Formen der Verschlüsselung zu wählen ist.

Eine wiederkehrende Frage ist: Was ist ein „Ende“? Wenn eine Mail-Adresse nicht personalisiert ist, sondern einer Funktion zugeordnet ist, dann ist ein solches Postfach zumeist von mehreren Personen zu nutzen, die einer spezifischen Gruppe angehören müssen. Ausschließlich Gruppenmitglieder haben Zugriff auf ein solches Postfach. Die 1:1-Beziehung zwischen den Teilnehmenden ist damit aufgelöst. Daher werden die E-Mails solcher so genannten Funktionspostfächer auf dem Mail-Server entschlüsselt. Das „Ende“ ist hier nicht mehr das Postfach der Teilnehmerin bzw. des Teilnehmers, sondern der Speicherort auf dem Mail-Server. Der befugte Zugriff erfolgt über eine besondere, dafür eingerichtete Prüfung. Die Prüfung kann z. B. über genau dafür zu verwendende Logins oder auch dafür zugeordnete, automatisierte Zugriffe (mittels „proxy user“) für eine Gruppe bzw. der zugeordneten Gruppenmitglieder realisiert werden. Die datenschutzkonforme Verarbeitung erfordert ein Gruppenmanagement, das auf einem validierten Rollen- und Rechte-Konzept basiert.

Von einer Ende-zu-Ende-Verschlüsselung kann weiterhin gesprochen werden,

- wenn der Mail-Server entsprechend gegenüber Angriffen z. B. durch geeignete Firewall-Technologien gesichert ist und sich im inneren Bereich des Netzwerks befindet, das von den Teilnehmenden innerhalb der eigenen PKI der IT-Abteilung genutzt wird;
- wenn das Rollen- und Rechte-System – genutzt für das erwähnte Gruppenmanagement – regelmäßig gegenüber den organisatorischen Strukturen der Unternehmen oder Organisationen validiert wird; und
- wenn insgesamt ein transparentes Verfahren für die Vergabe und den Entzug insbesondere der Gruppenrechte im Unternehmen oder der Organisation vorliegt.

5.1.1.8
Fazit

Ich freue mich über jede neue technische Idee und Lösung, die eine datenschutzkonforme Verarbeitung gewährleistet. Gleichzeitig ist festzustellen, dass permanent auf die Umsetzung der Gewährleistungsziele der Vertraulichkeit und Integrität hinzuweisen ist. Die Implementierungen sind auf diese Gewährleistungsziele zu prüfen. Denn die Verwendung von einer ggf. bestehenden PKI stellt nicht zwingend sicher, dass Transport- und Datensicherheit in entsprechender Weise umgesetzt sind. Daher empfehle ich dringend für jede erörterte Systemarchitektur im Einzelfall zu prüfen, ob die Interessen der Nutzenden gewahrt sind.

Die Nutzenden fordere ich weiterhin auf wachsam zu sein, ihren Anteil zu leisten, wie auch daran zu denken, für welche Zwecke sie ihre E-Mail-Adressen verwenden und wem sie ihre Kontaktdaten anvertrauen. Daher ist nochmals auf die Nutzung sowohl von Zertifikaten für Schlüsselpaare und digitale Signaturen aufmerksam zu machen. Selbstverständlich ist dafür zu sorgen, dass Mechanismen vorgesehen sind, mit denen die Zertifikate im laufenden Betrieb geprüft werden.

5.1.2
WhatsApp in der öffentlichen Verwaltung?

Im Laufe des Jahres erreichten mich Anfragen, ob nach den Änderungen bei der Verschlüsselung im Messenger WhatsApp eine dienstliche Nutzung in der Verwaltung möglich ist. Dieser Beitrag bezieht sich ausschließlich auf den öffentlichen Bereich. Wenngleich durch Einführung einer Verschlüsselung der Inhalte ein wesentlicher Beitrag zum Datenschutz und zur Datensicherheit erfüllt wurde, kann aus Sicht des Datenschutzes daraus noch nicht geschlossen werden, dass damit eine (uneingeschränkte) dienstliche Nutzung des Messengers möglich ist.

In 2016 hat WhatsApp die lange geforderte Verschlüsselung der Inhalte umgesetzt (vgl. z. B. die Erläuterungen in den WhatsApp-FAQ unter https://www.whatsapp.com/faq/de/general/28030015; Meldung im Heise-Newsticker vom 05.04.2016 unter https://www.heise.de/security/meldung/WhatsApp-Verschluesselung-fuer-alle-freigeschaltet-3163009.html; „Test: Hinter den Kulissen der WhatsApp-Verschlüsselung“ auf Heise-Security unter https://www.heise.de/security/artikel/Test-Hinter-den-Kulissen-der-WhatsApp-Verschluesselung-3165567.html; Links abgerufen am 24.10.2016).

5.1.2.1
Zu betrachtende Umstände

Weitere Umstände verbleiben, die eine Nutzung im dienstlichen Umfeld weiterhin problematisch machen:

Datenübertragung in die USA
Die in WhatsApp eingegebenen Daten werden im Rahmen der Nutzung auch auf Servern verarbeitet und gespeichert, die sich in den USA befinden. Nach der Aufhebung des Safe Harbor-Abkommens durch den EuGH und trotz des im Anschluss daraufhin vereinbarten Privacy Shield ist dies nach wie vor problematisch. Hinzu kommt noch die Übernahme von WhatsApp durch Facebook, die eine weitere Vermischung und gegenseitige Übertragung von Daten ermöglicht. Nach Änderung der Nutzungsbedingungen Ende August wurde im III. Quartal 2016 dies auch genutzt. Seit dem 09.11. setzte Facebook die Weitergabe von WhatsApp-Daten von europäischen Nutzerinnen und Nutzern auf Druck des Hamburger Datenschutzbeauftragten aus. Dieser Schritt bedeutet aber nicht, dass die Weitergabe dauerhaft unterbleibt.

Die Widerspruchsmöglichkeit bei der Annahme der geänderten Nutzungsbedingungen in WhatsApp war sehr versteckt untergebracht und zudem - nach unveränderter Annahme - nur innerhalb eines Zeitraums von 30 Tagen nach dieser Zustimmung noch möglich. Sofern dieser Zeitraum verstrichen ist, hat der Nutzer nunmehr keine Möglichkeit mehr, die Zustimmung zur Datenübertragung noch zu widerrufen.

Metadaten
WhatsApp verschlüsselt zudem nur die Inhaltsdaten der Kommunikation. Alle erforderlichen Metadaten zur Einrichtung, Aufrechterhaltung und Abwicklung der Kommunikation werden unverschlüsselt gespeichert und übertragen. Da WhatsApp zur Nutzung der uneingeschränkten Funktionalität insbesondere Zugriff auf das Telefonbuch verlangt, betrifft dies alle dort gespeicherten Daten auf dem Gerät.

Anmerkungen:
WhatsApp funktioniert auf Android-Geräten auch, wenn man der App den Zugriff auf das Telefonbuch verweigert, in diesem Fall werden anstelle der Namen - wie bei nicht im eigenen Telefonbuch gespeicherten Teilnehmern einer Kommunikation (WhatsApp-Gruppen) - lediglich die Nummern angezeigt.
Kein neuer WhatsApp-Kommunikationspartner oder keine neue WhatsApp-Kommunikationspartnerin kann angelegt werden, ohne dass ein Zugriff auf das Telefonbuch erfolgt.

Umsetzung der Inhaltsverschlüsselung
Trotz eines Verweises auf die Dokumentation des eingesetzten Verschlüsselungsalgorithmus bleibt in der Beschreibung offen, an welchem Ort der private Schlüssel des asymmetrischen Verfahrens gespeichert wird. Des Weiteren wird von einer „Kopie des privaten Schlüssels“ gesprochen, mit dem im Notfall die eigene Kommunikation mit jedem anderen Teilnehmer wiederhergestellt werden kann. Aus datenschutzrechtlicher Sicht darf es keine Kopie eines privaten Schlüssels außerhalb des Hoheitsbereiches des Inhabers geben; denn dann ist er nicht privat.

Auswertung der Kommunikation (Metadaten)
Unabhängig von der Verschlüsselung der ausgetauschten Nachrichten stimmen die Nutzenden der Auswertung ihrer Kommunikation für Marketingzwecke zu. In den AGBs wird nicht erklärt, welche Daten zu Marketingzwecken ausgewertet werden. Als sicher ist anzunehmen, dass die unverschlüsselten Metadaten genutzt werden. Des Weiteren ist bei der ungeklärten Frage nach einer möglichen Kopie des privaten Schlüssels auch die Auswertung der eigentlichen Kommunikation denkbar. Aus datenschutzrechtlicher Sicht wäre in diesem Fall keine Vertraulichkeit gewährleistet. Eine Nutzung von WhatsApp ist dann datenschutzrechtlich unzulässig, insbesondere wenn sensible Daten Inhalt der Kommunikation sein können.

5.1.2.2
Vergleich zu anderen Messenger-Diensten

Im Vergleich zu anderen, ebenso verfügbaren Messenger-Diensten, die die folgenden Kriterien erfüllen, ist von WhatsApp für eine datenschutzkonforme Nutzung, die die Interessen der Nutzenden wahrt, zu fordern:

1. Die ausgetauschten Nachrichten sind zu hashen und für jeden Nutzenden getrennt zu speichern.
2. Es bedarf strikter Regelungen für Zugriffsmechanismen, die Interessen der Nutzenden wahren.
3. Eine Weitergabe von Kontakten ist nicht gestattet, wie ausführlich erläutert.
4. Eine Weitergabe und Auswertung von Metadaten an andere ist nicht gestattet, wie bereits beschrieben. Dazu gehören auch andere Unternehmensteile im Konzern.
5. Ein Zugriff durch eine begrenzte Anzahl von Systemadministratoren ist ebenso zu regeln.

Die angegebenen Kriterien entsprechen im Wesentlichen den Forderungen, die auch von der Artikel 29-Gruppe europaweit an WhatsApp gestellt werden. Federführend für die Durchsetzung der Anforderungen ist die „Subgroup Enforcement“ der schon genannten Artikel 29-Gruppe, die auch die Forderungen im Dezember 2016 veröffentlicht hat.

5.1.2.3
Abwägungen und Prüfbarkeit

Diese genannten Problemfelder stehen grundsätzlich einer Nutzung im Umfeld der Verwaltung entgegen. Die Datenschutzaufsichtsbehörden des Bundes und der Länder sowie die Aufsichtsbehörde für Telekommunikationsdienstleistungs-Unternehmen (Bundesnetzagentur) sind der Auffassung, dass es sich bei so genannten „over the top“-Diensten – wie WhatsApp –, um eine Telekommunikationsdienstleistung im Sinne des Telekommunikationsgesetzes handelt. Das bedeutet, dass mit einem solchen Telekommunikationsdienstleister kein Vertrag über die Verarbeitung personenbezogener Daten im Auftrag gemäß § 4 HDSG zu schließen ist. Gleichwohl werden Kontaktdaten und Metadaten durch WhatsApp für eigene Zwecke verarbeitet.

Aus diesem Grund halte ich die Nutzung von WhatsApp durch die öffentliche Verwaltung in der Regel nicht für datenschutzkonform. Eine Nutzung kann nur u. U. in Ausnahmefällen vertretbar sein, bei denen eine nachprüfbare Interessenabwägung zwischen Zielerreichung und Schutz der Betroffenenrechte trotz aller datenschutzrechtlichen Bedenken für den Einsatz von WhatsApp spricht, um ein höherrangiges Ziel zu wahren, z. B. die Möglichkeit der Kontaktaufnahme mit Jugendlichen im Bereich der Jugendhilfe, wenn andere Kanäle nicht zur Verfügung stehen.

Derartige Ausnahmen sind immer streng zu prüfen. Im Rahmen der Vorabkontrolle ist festzustellen und zu begründen, ob für den geplanten Zweck ein Messenger-Dienst überhaupt erforderlich ist. Wenn ja, ist der Messenger-Dienst auszuwählen, der die Anforderungen des Datenschutzes im Rahmen der vorgesehenen Nutzung am besten erfüllt. Hier bietet der Markt mittlerweile auch datenschutzfreundliche Alternativen zu WhatsApp (z. B. Threema o. Ä.), deren Nutzung zu bevorzugen ist.

Ergibt die Abwägung dennoch eine zwingende Erforderlichkeit für das Produkt WhatsApp, müssen für den Einsatz zusätzlich die folgenden Rahmenbedingungen zum Schutz von Betroffenenrechten eingehalten werden:

1. **Dienstliches Gerät**
   Die Nutzung ist nur auf dienstlichen Geräten zulässig, da nur hier sowohl ein entsprechendes Sicherheitsniveau und -umfeld geschaffen werden kann (Device Management, Kontrolle der installierten Apps usw.) als auch ein separates Adressbuch vorhanden ist. Die Behörde muss möglichst mit einer Funktions-ID auftreten.

2. **Adressbuch**
   Auf dem Gerät dürfen nur Daten von Kommunikationspartnern gespeichert werden, die zur Abwicklung der vorgesehenen Kommunikationsbeziehungen erforderlich sind. Insbesondere muss sichergestellt werden, dass Daten von Kontakten, die einer Nutzung von WhatsApp nicht explizit zugestimmt haben, nicht auf dem Geräte-Telefonbuch abgespeichert werden.

3. **Alternative Kommunikationswege**
   In dem Bereich, in dem WhatsApp zur Kommunikation verwendet werden soll, ist in jedem Fall ein alternativer Kommunikationsweg aufzubauen bzw. aufrechtzuerhalten, um eine Kontaktaufnahme außerhalb von WhatsApp zu ermöglichen.

4. **Nutzung durch Dritte**
   Der Kommunikationskanal WhatsApp ist in den betroffenen Bereichen in aller Regel als schneller Kommunikationsweg gedacht (z. B. im Bereich der Abfallwirtschaft, wenn es um wilde Müllablagerungen geht). Sofern WhatsApp als alternativer Kommunikationsweg durch die Verwaltung publiziert wird, kann bei Eröffnung der Kommunikation durch Dritte (d. h. von außen) implizit von einer Einwilligung zur Nutzung von WhatsApp für Antworten/Rückfragen ausgegangen werden. Insofern ist eine Speicherung der Kommunikationsdaten zulässig – die Daten sind aber unverzüglich zu löschen, wenn Dritte dies explizit verlangen. In diesem Fall darf auch WhatsApp zur Kommunikation mit den betreffenden Personen durch die Verwaltung nicht mehr genutzt werden.

Die Vorabkontrolle und damit die genannten Kriterien 1 bis 4 sind überprüfbar, so dass sowohl im Betrieb von der verantwortlichen Stelle eine regelmäßige Kontrolle zu erfolgen hat als auch diese Kriterien von der Aufsichtsbehörde geprüft werden.

5.2
Videoüberwachung

5.2.1
Videoüberwachung nach Bundesdatenschutzgesetz

Die Videoüberwachung nach dem Bundesdatenschutzgesetz ist nach wie vor ein Dauerbrenner in meiner Behörde.

Die Fallzahlen haben sich auf einem konstant hohen Niveau stabilisiert. Auch im aktuellen Berichtszeitraum waren daher beratende Tätigkeiten bzw. mein Eingreifen geboten, um datenschutzrechtlichen Verstößen vorzubeugen bzw. bei entsprechenden Verstößen auf die Einhaltung datenschutzrechtlicher Vorschriften hinzuwirken.

Erfreulich ist die Tatsache, dass mittlerweile eine zunehmende Zahl von Kamerabetreibern vor der Installation von Überwachungskameras eine Beratung hinsichtlich der Zulässigkeit einer (geplanten) Überwachungsmaßnahme anfragt, sodass bereits von vornherein eine datenschutzrechtlich zulässige Installation der Überwachungskameras erfolgen kann.
Eine entsprechende „Beratungswelle“ erreichte mich im Winter 2015/2016, als die Zahl der Wohnungseinbrüche hessen- und deutschlandweit enorm anstieg.

Bei einem Großteil der Eingaben fiel nach wie vor die Unwissenheit darüber auf, dass öffentliche Bereiche nicht bzw. nur im Rahmen des § 6b BDSG überwacht werden dürfen. Zumeist ging es um den klassischen Nachbarschaftsstreit. Insoweit beziehe ich mich auf die Ausführungen in meinem 44. Tätigkeitsbericht (Ziff. 4.9.1).

Im Berichtszeitraum konnte generell in Fällen – wenn auch in Einzelfällen erst nach Androhung und Festsetzung eines Zwangsgeldes – ein datenschutzkonformer Betrieb der jeweiligen Überwachungsmaßnahme erreicht werden.

5.2.2
Videoüberwachung der Gefahrenabwehrbehörden

Auch in diesem Jahr wurde ich von öffentlichen Stellen um Beratung zu unterschiedlichsten Projekten der Videoüberwachung gebeten.

5.2.2.1
Rechtliche Grundlagen

Ein Einsatz einer Videoüberwachungsanlage ist immer nur auf Grundlage einer konkreten gesetzlichen Ermächtigung zulässig. Denn er stellt immer auch einen Eingriff in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung dar. Für hessische öffentliche Stellen ergibt sich der Beurteilungsmaßstab aus § 14 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG).

§ 14 Abs. 4 HSOG regelt die offene Videoüberwachung durch Gefahrenabwehrbehörden, in der Regel damit durch kommunale Ordnungsbehörden. Gemäß § 14 Abs. 4 Nr. 1 HSOG ist für die Gefahrenabwehrbehörden hier ausschließlich die offene Videoüberwachung an Orten, an denen wiederholt Straftaten begangen worden sind und tatsächliche Anhaltspunkte für weitere Straftaten bestehen, zulässig.

§ 14 Abs. 3 und 4 HSOG

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

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

1. zur Sicherung öffentlicher Straßen und Plätze, auf denen wiederholt Straftaten begangen worden sind, sofern tatsächliche Anhaltspunkte für weitere Straftaten bestehen,
2. zum Schutz besonders gefährdeter öffentlicher Einrichtungen,
3. zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.

Gefahrenabwehrbehörde im Sinne der Nr. 2 ist auch der Inhaber des Hausrechtes. Abs. 1 Satz 2 und 3, Abs. 3 Satz 2 und 3 sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend.

Die Videoüberwachung bleibt zur Verhinderung von Straftaten und zur Erhöhung des subjektiven Sicherheitsgefühls verstärkt Teil der politischen und öffentlichen Diskussion. Die immer günstiger zu beschaffende und unterhaltende Technik wird insbesondere dort gewünscht, wo personelle Ressourcen knapp sind.

5.2.2.2
Beurteilung der Anfragen von Kommunen zu Kriminalitätsbrennpunkten

Regelmäßig wenden sich Kommunen mit Fragen zur Einrichtung von Videoüberwachungsanlagen an mich, nachdem es entweder an bestimmten Orten zu subjektiv wahrgenommenen Häufungen von Kriminalität gekommen ist oder Bereiche aufgrund ihrer Lage oder Ausgestaltung von Bürgern als Angsträume wahrgenommen werden. Tatsächlich vermitteln oftmals Unterführungen insbesondere zu wenig frequentierten Zeiten ein Gefühl des Ausgeliefertseins für den Bürger und bieten günstige Tatgelegenheitsstrukturen für Täter. Letztere nachteilig zu beeinflussen und das Entdeckungsrisiko für den Täter zu erhöhen, ist das primäre Ziel der offenen Videoüberwachung nach § 14 Abs. 4 Nr. 1 HSOG als präventive Maßnahme.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung muss verhältnismäßig zum angestrebten Erfolg sein. Dabei ist zu bedenken, dass eine Vielzahl von Personen zwangsläufig der Datenerhebung unterworfen werden, wenn sie die überwachte Örtlichkeit aufsuchen. Zweifellos wird manch potenzieller Täter vor dem Hintergrund eines höheren

Entdeckungs- und Verfolgungsrisikos offen videoüberwachte Örtlichkeiten meiden, wenngleich auch nicht gänzlich Abstand von seinem Vorhaben nehmen. Die offene Videoüberwachung führt demnach nur zu einem Rückgang der Kriminalität im konkreten Bereich der videoüberwachten Örtlichkeit. Auch dies ist daher in die Überlegungen zur Verhältnismäßigkeit des Einsatzes mit einzubeziehen.

Die rechtlichen Voraussetzungen für die Gefahrenabwehrbehörden nach § 14 Abs. 4 Nr. 1 HSOG erfordern eine retrograde Beurteilung der Kriminalität sowie eine Kriminalitätsprognose für den vorgesehenen Standort der Videoüberwachungsanlage. Zur Bewertung und Darstellung der Kriminalität ist die Betrachtung der polizeilich erhobenen Daten zu Straftaten unumgänglich. Für Auswertungen kann hier die polizeiliche Kriminalstatistik herangezogen werden. Seitens der zuständigen Polizei sollte ergänzend das Kriminalitätslagebild nach § 20 Abs. 9 HSOG ausgewertet werden, um die erfolgte Kriminalität am geplanten Standort darzustellen. Bei dem Standort der Videoüberwachung soll es sich um einen relativen Kriminalitätsschwerpunkt handeln, er muss also vergleichend betrachtet werden, wobei natürlich auch die jeweiligen Tatgelegenheitsstrukturen und kriminalgeografischen Gegebenheiten bewertet werden müssen, die an einem Einkaufszentrum völlig anders sind als beispielsweise einem Bahnhof oder in einem Wohnviertel.

Weiterhin ist zu beachten, dass sich nur ein bestimmter Kriminalitätsbereich durch offene Videoüberwachung beeinflussen lässt, als typisch wäre hier die Straßenkriminalität zu nennen, also Straftaten mit Tatort auf öffentlichen Wegen, Straßen oder Plätzen. Straftaten im häuslichen oder geschäftlichen Bereich gehören regelmäßig nicht zu den Straftaten, die sich durch eine präventive Videoüberwachung im öffentlichen Bereich verhindern lassen und sollten daher auch nicht in die Darstellung eines Kriminalitätsschwerpunktes einbezogen werden.

5.2.2.3

Anfragen zum Schutz besonders gefährdeter öffentlicher Einrichtungen

Eine weitere Möglichkeit des offenen Einsatzes der Videoüberwachung besteht nach § 14 Abs. 4 Nr. 2 HSOG „zum Schutz besonders gefährdeter öffentlicher Einrichtungen“. In diesem Kontext gibt es sehr unterschiedliche Anfragen aus Kommunen. Bei Anfragen im Kontext der Sicherung größerer Flüchtlingsunterkünfte der Erst- oder Zweitaufnahme habe ich mich im Laufe des Jahres veranlasst gesehen, hier eine besondere Gefährdung zu bejahen, nachdem es seit der angestiegenen Aufnahme von Flüchtlingen an zahlreichen Flüchtlingsunterkünften in Deutschland zu Straftaten kam, die sich konkret gegen die Einrichtung und ihre Bewohner richteten.

Gegenstand von Anfragen der Kommunen zu Videoüberwachungen sind jedoch auch vermehrt Einrichtungen wie Kindergärten, Kindertagesstätten und Sportplätze, die außerhalb der jeweiligen Öffnungszeiten Ziel von Vandalismus oder auch nur Verunreinigungen werden, ohne dass die rechtlichen Voraussetzungen nach § 14 Abs. 4 Nr. 1 HSOG vorliegen. Die Nutzung der Einrichtungen wird daher zumindest zeitlich eingeschränkt, Aufwand und Kosten für z. B. Reinigungen werden nötig.

Bei den beispielhaft genannten öffentlichen Einrichtungen kann man eine grundsätzliche „besondere Gefährdung“ nicht bejahen. Trotzdem könnte hier oft eine offene Videoüberwachung ein geeignetes Mittel zur Prävention sein. Vergleichbare private Einrichtungen können in solchen Situationen auf Grundlage des § 6b BDSG als Hausrechtsinhaber Videoüberwachungsanlagen betreiben. Ich habe daher wiederholt angeregt, dass der hessische Gesetzgeber eine vergleichbare Regelung schafft, die es unter Abwägung des Rechts der Bürgerinnen und Bürger auf Zugang zu öffentlichen Einrichtungen und andererseits dem Interesse auf Verhinderung von massiven Schäden, die auch die öffentlichen Haushalte belasten, ermöglicht, auch Videotechnik einzusetzen.

5.2.2.4

Organisation der Hinweispflicht auf die Überwachung

Durch Bürgereingaben, aber auch aus eigenen Feststellungen fällt immer wieder auf, dass der Hinweispflicht gemäß § 14 Abs. 3 Satz 2 bzw. § 14 Abs. 4 Satz 3 HSOG für offene Videoüberwachungen in der Form Rechnung getragen wird, dass man an den jeweiligen Kameras entsprechende Hinweistafeln anbringt. Zweck der Vorschrift ist jedoch nicht die Kennzeichnung einer Kamera, sondern des überwachten Bereichs. Es soll erkennbar sein, dass man sich nun in einen videoüberwachten Bereich begibt und ihn damit alternativ und ohne aufgezeichnet zu werden meiden/umgehen kann. Eine Kennzeichnung unmittelbar an der Kamera ist nicht zielführend und kann daher der gesetzlichen Kennzeichnungspflicht nach § 14 Abs. 3 Satz 2 HSOG keinesfalls genügen.

6. Querschnitt – Gesundheitswesen im öffentlichen und nicht-öffentlichen Bereich

6.1

Übergabe der Patientenkartei an einen Praxisnachfolger

Häufig erreichen mich Eingaben zu der Frage, was mit den Patientendaten passiere, wenn ein Arzt seine Praxis aufgibt. Auch im folgenden Fall erhielt ich eine Eingabe betreffend die Aufbewahrung der Patientenakte durch einen Praxisnachfolger.

6.1.1

Sachverhalt

Anlässlich einer Terminanfrage bei seiner bisherigen Praxis teilte man dem Eingebenden mit, dass seine Ärztin die Praxis aufgegeben habe und seine Patientendaten „an eine andere Gemeinschaftspraxis“ weitergegeben worden seien. Für den Eingebenden war diese kurze Mitteilung nicht nachvollziehbar und er bat mich um Überprüfung, ob es zulässig gewesen sei, die Patientendaten ohne seine Erlaubnis an einen neuen Arzt zu übergeben.

Ich habe daraufhin mit der ehemaligen Ärztin Kontakt aufgenommen. Diese hatte zum Ende des Jahres 2015 ihre Praxis in Hessen aufgegeben und war in ein anderes Bundesland verzogen. Ihr bisheriger Arztsitz ging an zwei Ärzte. Über die bevorstehende Praxisaufgabe und die Nachfolger informierte die Ärztin ihre Patienten auf ihrer Homepage und in der regionalen Tageszeitung.

Im Rahmen des Praxisverkaufs wurden auch vertragliche Regelungen zur Verwahrung der Patientenakten mit den übernehmenden Ärzten getroffen. Man einigte sich darauf, die ehemaligen Patientenakten zwischen den beiden Nachfolgern aufzuteilen. Dabei erfolgte eine Aufteilung nach Jahrgängen. Da der eine Arzt in der gleichen Fachrichtung wie die bisherige Ärztin praktizierte, erhielt er alle aktuellen Patientenakten einschließlich der elektronischen Dokumentation, da man annahm, die ehemaligen Patienten würden sich dort in die Weiterbehandlung begeben (Jahrgänge 2011 bis 2015). Die Ärztin, die die bisherigen Praxisräume bezog, erhielt alle Akten der Patienten, die länger nicht mehr in Behandlung waren und die aufgrund geltender Aufbewahrungsfristen noch nicht vernichtet werden durften (Jahrgänge 2006 bis 2010).

Beide Käufer verpflichteten sich, die Patientenakten in einem separaten Aktenschrank zu verwahren und nur mit einer schriftlichen Einwilligung des jeweiligen Patienten auf die Akten zuzugreifen.

Ich habe Anfang 2016 die beiden Arztpraxen besucht und geprüft, wie die vertraglichen Regelungen praktisch umgesetzt wurden.

6.1.2

Feststellungen vor Ort und getroffene Maßnahmen

Beim Besuch der ersten Praxis wurde festgestellt, dass das gängige „Zwei-Schrank-Modell“ umgesetzt wurde, soweit die Papierakten betroffen sind. Laut Auskunft meines Ansprechpartners der Gemeinschaftspraxis wird demnach auf die übernommene, separat verwahrte Patientenakte nur zugegriffen, wenn der betreffende Patient seine Einwilligung hierzu erklärt. Ein Einwilligungsformular, mit dem dies dokumentiert wird, wurde mir bei meinem Besuch vorgelegt. Zugleich hatte man ein Ablaufprotokoll für das Praxispersonal angefertigt, das den Umgang mit den übernommenen Akten regelt. So haben insbesondere nur ausgewählte, klar benannte Mitarbeiter Zugriff auf die Akten.

Darüber hinaus wurde die komplette Praxis-EDV von dieser Praxis übernommen, so dass auch die elektronischen Daten zu den Akten, die sich in der anderen Praxis befinden, hier aufbewahrt werden. Diesbezüglich habe ich die Frage der Zulässigkeit aufgeworfen. Bislang wurde der Umgang mit diesen Daten so gehandhabt, dass diese passwortgeschützt auf dem alten Rechner der Praxisvorgängerin gespeichert bleiben und nur auf entsprechende Anfrage des jeweiligen Patienten hin dessen Daten abgerufen werden. Durch meinen Besuch konnte es gerade noch rechtzeitig vermieden werden, dass man die Daten ungefiltert in die eigene Praxis-EDV übernahm.

Im Hinblick auf die zweite besuchte Praxis stellte sich schließlich das Problem, dass die Ärztin, die die Akten der Vorgängerin übernommen hat, einer anderen Fachrichtung angehört. Dies bedeutete, dass die Patienten der ehemaligen Ärztin im Grunde bereits von vornherein nicht von der Nachfolgerin weiterbehandelt werden konnten. Tatsächlich teilte die Ärztin mit, dass sie in der Regel lediglich die Akten der Vorgängerin herausgebe und einen entsprechenden Spezialisten auf dem Gebiet der Vorgängerin empfehle. Auch hier stellte sich wiederum die Frage, ob dies nach dem Grundgedanken des „Zwei-Schrank-Modells“ zulässig ist. Letztlich ist es hier bereits im Vorfeld gar nicht nötig, dass der Praxisnachfolgerin die Möglichkeit der Kenntnisnahme gegeben wird, da sie ohnehin auf einem anderen Fachgebiet tätig ist.

Bei meinem Besuch der zweiten Praxis wurde ferner festgestellt, dass die Patientenakten der Praxisvorgängerin (Jahrgänge 2006 bis 2010) noch in Umzugskartons lagerten und damit nicht ordnungsgemäß getrennt von der eigenen Patientendokumentation auf dem Dachboden untergebracht waren. Es wurde mir jedoch eine zeitnahe, ordnungsgemäße Unterbringung in separaten, verschließbaren Metallschränken zugesagt. Dies hat man mir gegenüber mittlerweile auch mittels Lichtbildern nachgewiesen.

Eine Dienstanweisung für das Praxispersonal bezüglich des Umgangs mit den Altakten wurde auf mein Anraten hin erstellt.

6.1.3

Dialog mit der Landesärztekammer Hessen zu den offenen Fragen

Im Folgenden habe ich noch einmal die offenen Fragen mit der Landesärztekammer Hessen erörtert. Im Ergebnis bin ich der Ansicht, dass eine Aufteilung der Patientendokumentation nach Jahrgängen nicht zielführend und auch im Hinblick auf den Grundsatz der Datensparsamkeit als problematisch einzustufen ist. Im vorliegenden Fall bin ich jedoch davon ausgegangen, dass eine Umorganisation der Aufteilung der Patientendokumentation nur mit unverhältnismäßig hohem Aufwand möglich ist, weshalb ich von weiteren Maßnahmen abgesehen habe. Ich habe jedoch darauf hingewiesen, dass dies im Falle einer künftigen Praxisübergabe zu beachten ist.

Thematisiert wurde von mir auch noch einmal, ob die Übernahme der Patientendokumentation auch durch einen fachfremden Arzt erfolgen kann, der keine Einsicht in die Dokumentation nimmt und sie lediglich verwahrt. Ein datenschutzrechtlicher Verstoß ist hier jedoch bereits deshalb nicht gegeben, da keine Verarbeitung personenbezogener Daten erfolgt, ohne dass der Patient diese veranlasst hat. Von Kammerseite wurden diesbezüglich auch keine berufsrechtlichen Bedenken geäußert.

Des Weiteren vertrete ich den Standpunkt, dass eine Einsichtnahme im Rahmen des „Zwei-Schrank-Modells“ auch bei der digitalen Patientendokumentation erst erfolgen darf, wenn hierfür die Einwilligung des Patienten vorliegt. Eine vorzeitige, ungefilterte Übernahme der Patientendaten in die Praxis-EDV ist daher aus datenschutzrechtlicher Sicht und auch vor dem Hintergrund des § 203 StGB unzulässig.

Ich habe die Landesärztekammer Hessen darauf hingewiesen, dass mir einige ihrer Mitglieder mitgeteilt haben, dass sie sich Informationen und Handreichungen zu der Frage wünschen, wie mit elektronischen Daten von Praxisvorgängern zu verfahren ist. Ich werde speziell zu diesem Themenkomplex auch weiterhin mit der Landesärztekammer Hessen im Dialog bleiben.

6.2

Datenschutzverstöße aus dem Bereich der Arztpraxen

Immer wieder führt ein leichtfertiger Umgang mit Patienten- bzw. Behandlungsdaten im Alltagsgeschäft von Arztpraxen zu Beschwerden. Hier zwei Sachverhalte, die im Berichtsjahr Anlass dazu gegeben haben, ein Bußgeldverfahren einzuleiten, mit mehr Sorgfalt aber zu verhindern gewesen wären.

6.2.1

Übersendung von Erinnerungs-E-Mails an Patienten mittels Nutzung eines offenen Verteilers

Bei der zugrunde liegenden Eingabe informierte mich der Patient eines Zahnarztes darüber, dass er alle sechs Monate per E-Mail an den nunmehr fälligen Kontrollbesuch erinnert wird. Im Falle einer solchen aktuellen Erinnerungsmail fiel dem Patienten auf, dass im E-Mail-Verteiler noch 27 weitere Empfänger der Daten angeführt waren. Die E-Mail-Adressen enthielten dabei zum überwiegenden Teil auch den Vornamen und den Nachnamen des Nutzers. Der Eingebende bemängelte, dass nun alle Empfänger wissen, welchen Zahnarzt er besucht und dass er dort seit über sechs Monaten nicht erschienen ist. Der Eingebende bat im Übrigen daraufhin die Zahnarztpraxis seine E-Mail-Adresse zu löschen und keine weiteren E-Mails zu senden, die seine vollständige E-Mail-Adresse enthalten. Eine Antwort auf diese Bitte erhielt er nicht.

Ich habe die betroffene Zahnarztpraxis zunächst um Stellungnahme gebeten. Hierbei wurde noch einmal darauf hingewiesen, dass die verschickte E-Mail insgesamt 27 E-Mail-Adressen von anderen Patienten aus der Praxis enthielt. Aus meiner Sicht bedeutet dies grundsätzlich einen Verstoß gegen die ärztliche Schweigepflicht, zumal einige der E-Mail-Adressen die Klarnamen von Patienten aufwiesen.

Die Zahnarztpraxis wurde von meiner Seite außerdem darüber aufgeklärt, dass im gegebenen Fall auch ein Verstoß gegen § 43 Abs. 2 Nr. 1 BDSG im Raum steht, da es sich bei E-Mail-Adressen um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG handelt. Es ist insoweit nicht einmal zwingend erforderlich, dass die E-Mail-Adresse aus einem Vor- und einem Nachnamen besteht.

Die Zahnarztpraxis teilte mir daraufhin mit, dass es sich bei dem Vorgang um ein Versehen gehandelt habe. Dieses Versehen sei auf das Handeln einer stets zuverlässigen und verantwortungsvollen Mitarbeiterin zurückzuführen. Diese habe die Erinnerung an anstehende Zahnarzt- oder Kontrolltermine parallel an die E-Mail-Adressen mehrerer Patienten gleichzeitig versandt.

Im Ergebnis blieb mir jedoch trotz des Bedauerns der verantwortlichen Stelle keine andere Möglichkeit, als ein Bußgeldverfahren einzuleiten. Zu berücksichtigen war hier insoweit, dass, auch wenn es sich um einen erstmaligen Verstoß handelte, im konkreten Fall eine Vielzahl an Patienten betroffen war. Insbesondere fanden sich unter den 27 im E-Mail-Verteiler genannten E-Mail-Adressen auch mindestens 18, die über die Vor- und Nachnamen eine direkte Zuordnung zu einer Person zuließen. Bereits der Umstand, dass eine bestimmte Person die Praxis des Zahnarztes besucht hat, fällt unter den Bereich der ärztlichen Schweigepflicht.

Im Nachgang habe ich mir im Übrigen noch einmal den Aufnahmebogen der Zahnarztpraxis genauer angesehen, mittels dessen in die Benachrichtigung und Erinnerung an Kontrolluntersuchungen/Prophylaxetermine eingewilligt werden kann. Das Formular sah insoweit die Erinnerung „per Telefon, per Postkarte oder per E-Mail“ vor. Diesbezüglich habe ich darauf hingewiesen, dass die Variante mittels Postkarte ausscheidet. Hier ist zu berücksichtigen, dass andernfalls ein besonders sensibles Datum offen zugänglich verschickt wird. Zwar kann eine im gleichen Haushalt lebende Person unter Umständen auch einem Briefumschlag entnehmen, dass die betroffene Person bei dem genannten Arzt in Behandlung war, die zusätzliche Angabe, weshalb das Anschreiben erfolgt, ist jedoch nicht von außen ersichtlich. Die Variante Erinnerung „per Postkarte“ war daher durch die Variante Erinnerung „per Brief“ zu ersetzen.

6.2.2

Weitergabe von Behandlungsdaten an eine externe Abrechnungsstelle und an einen Rechtsanwalt ohne Einwilligung des Patienten

In regelmäßigen Abständen erhalte ich auch immer wieder Hinweise von Patienten, dass deren Behandlungsdaten ohne das Einholen einer entsprechenden Einwilligung an eine externe Abrechnungsstelle weitergeleitet wurden. Auch in einem Fall aus dem letzten Berichtsjahr hat eine Arztpraxis dies mir gegenüber eingeräumt. Der Eingebende bemängelte darüber hinaus, dass die Arztpraxis seine Behandlungsakte auch in vollem Umfang an einen beauftragten Rechtsanwalt weitergegeben habe. Als Hintergrund hierfür teilte mir die Arztpraxis mit, dass der Eingebende gegenüber dem behandelnden Arzt erklärt habe, er wolle die Rechnung nicht bezahlen, sondern eine Verrechnung mit ihm zustehenden Schadensersatzansprüchen vornehmen.

Für die Frage, ob und in welchem Umfang Behandlungsdaten an einen Rechtsanwalt übermittelt werden können, kommt es entscheidend darauf an, inwieweit diese zur Aufgabenerfüllung erforderlich sind. Die vollständigen Behandlungsunterlagen dürfen nur dann übergeben werden, wenn dies der jeweilige Zweck tatsächlich erfordert. Dies ist beispielsweise nicht der Fall, wenn der Rechtsanwalt eine Honorarforderung aus einer Behandlung aus dem Jahr 2012 durchsetzen soll, ihm dabei aber zugleich Informationen zu Behandlungen übersandt werden, die neun Jahre zuvor stattgefunden haben. Einen derartigen Fall habe ich entsprechend auch als grundsätzlich bußgeldwürdig eingestuft. In der gegebenen Situation habe ich die Sachlage jedoch anders gesehen. Bei einer eindeutigen Aussage, man wolle den Behandlungsbetrag nicht bezahlen und zugleich mit Schadensersatzansprüchen aufrechnen, ist die Einsichtnahme in die komplette Behandlungsakte aus datenschutzrechtlicher Sicht vertretbar. Dies steht auch nicht im Widerspruch zu der Rechtsprechung des Bundesgerichtshofes (siehe beispielsweise BGH, Urteil vom 23.06.1993, Az.: VIII ZR 226/92). Danach ist der Arzt zu einer sorgfältigen, am Grundsatz der Verhältnismäßigkeit ausgerichteten Abwägung zwischen seinen eigenen berechtigten wirtschaftlichen Interessen und dem Geheimhaltungsbedürfnis des Patienten angehalten. Die Preisgabe von Behandlungsdaten hat er insoweit auf das angemessene, für die Beitreibung seiner Honoraransprüche erforderliche Maß zu beschränken. Ein entsprechendes Korrektiv sieht auch § 28 Abs. 6 Nr. 3 BDSG vor („… und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt“).

Im Ergebnis blieb damit nur das Weiterleiten von Behandlungsdaten an die externe Abrechnungsstelle als bußgeldwürdiger Sachverhalt bestehen.

6.3
Unsachgemäße Entsorgung von Implantationsprotokollen

Implantationsprotokolle eines Herstellers von Implantaten, die anlässlich von Operationen u. a. zur Qualitätssicherung erstellt werden, müssen datenschutzgerecht vernichtet werden.

Ein in Hessen ansässiger Produzent von Implantaten meldete mir vorsorglich einen Datenschutzvorfall nach § 42a BDSG. Es wurde mitgeteilt, dass eine Außendienstmitarbeiterin, wohnhaft in NRW, Transplantationsprotokolle mit Patientendaten ungeschreddert im regulären Papiermüll entsorgen wollte. Offenbar hatte eine weitere Person dies beobachtet und der Mitarbeiterin die Kartons mit den entsprechenden Unterlagen wieder direkt vor die Haustür gestellt. Zugleich erging eine Meldung an die zuständige Kreispolizeibehörde, die ihrerseits die Unterlagen sicherstellte und zugleich ordnungsgemäß vernichtete.

Im Hinblick auf den geschilderten Fall ging es zunächst um die Bewertung, ob von dem Unternehmen eine vorsorgliche Meldung gemäß § 42a BDSG auch an die betroffenen Patienten erfolgen muss oder ob aufgrund der gegebenen Besonderheiten hiervon abgesehen werden konnte. Das Unternehmen ließ sich dahingehend ein, dass die Informationspflicht gemäß § 42a BDSG über die Kenntniserlangung durch einen Dritten hinaus voraussetze, dass den Betroffenen schwerwiegende Beeinträchtigungen für ihre rechts- oder schutzwürdigen Interessen drohen.

> § 42a BDSG
>
> Stellt eine nicht-öffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte
> 1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
> 2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
> 3. ...
> 4. ...
>
> 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 mitzuteilen.
> ...

Dies sei im vorliegenden Fall nicht zu bejahen, zumal lediglich Polizeibeamte Kenntnis von den Unterlagen erhalten hätten und die Unterlagen zwischenzeitlich vernichtet wurden. Diesbezüglich wurde von meiner Seite eingewandt, dass zumindest eine unbekannte Person die Kartons mit den Implantationsprotokollen vom Papiercontainer entfernt und der Mitarbeiterin vor die Haustür gelegt hatte. Damit war es zumindest einer weiteren Person möglich, für einen gewissen Zeitraum auf die Protokolle zuzugreifen und hier unter Umständen auch einzelne Dokumente zu entwenden. Zugleich war auch nicht auszuschließen, dass weitere Personen die Papiercontainer aufsuchten und dort einzelne Protokolle entwendeten. Letztlich war für eine weitere Bewertung für mich von Bedeutung, für wie lange sich die Dokumente frei zugänglich am Papiercontainer und vor der Haustür der Mitarbeiterin befanden.

Hierzu wurde mir mitgeteilt, dass sich die Protokolle für maximal 18 Stunden außerhalb der Obhut des Unternehmens befanden. So habe die Mitarbeiterin diese gegen 18:00 Uhr an einem Sonntagabend vor dem Papiercontainer abgelegt. Bereits am darauffolgenden Montag haben sich die Unterlagen zwischen 11:00 Uhr und 11:30 Uhr wieder vor ihrer Haustür befunden. Nach den Recherchen waren insgesamt 100 Implantationsprotokolle betroffen, die zum Teil detaillierte Angaben zum Operationsvorgang enthielten. Zugleich war die Besonderheit gegeben, dass die Mitarbeiterin die Durchschläge mit Patientenaufklebern versehen habe, was grundsätzlich so nicht vorgesehen sei. Insgesamt gäbe es zu den Protokollen drei Durchschläge. Das Original mit Patienteninformationen verbleibe beim Krankenhaus, ein Durchschlag ohne diese Informationen erhalte die Mitarbeiterin, die während der Operation im Krankenhaus zugegen ist. Ein weiteres Exemplar, ebenfalls ohne Informationen zum Patienten, sei für das Unternehmen bestimmt.

Als weitere Schwierigkeit stellte sich heraus, dass die Unterlagen bereits durch die Kreispolizeibehörde vernichtet wurden, so dass keine Daten zu den tangierten Personen mehr vorlagen. Das Unternehmen hätte zur Abklärung, welche Personen betroffen sind, zunächst den Weg über die Krankenhäuser gehen müssen.

Im Ergebnis wurde im Hinblick auf die Meldung nach § 42a BDSG vorgetragen, dass der für die erstmalige Identifikation der Betroffenen nötige Aufwand im Hinblick auf den minimalen Nutzen einer Unterrichtung als auch die Abwesenheit einer plausiblen Gefährdungslage nicht verhältnismäßig sei. Ergänzend wurde darauf hingewiesen, dass die Implantationsprotokolle nicht mitarbeiterbezogen aufgehoben würden. Es müssten insoweit alle für die Jahre 2012 und 2013 vorhandenen Durchschläge nach diesem Kriterium durchsucht werden. Den Angaben nach handelt es sich hierbei um ca. 20.000 Protokolle. Als Weiteres müssten die jeweiligen Krankenhäuser angeschrieben werden und so die Verbindungen zum konkreten Patienten hergestellt werden.

Angesichts dieser Schilderung war von meiner Seite noch einmal zu berücksichtigen, dass sich die Dokumente tatsächlich nur für achtzehn Stunden außerhalb des Gewahrsams des Unternehmens befanden und die Identifikation der Patienten mit einem nicht unerheblichen Aufwand verbunden war. Angesichts dieser Umstände habe ich es für vertretbar gehalten, von einer Verpflichtung zur Unterrichtung nach § 42a BDSG abzusehen. Dies galt natürlich nur unter dem Vorbehalt, dass nicht weitere Anhaltspunkte darauf hinweisen, dass tatsächlich Unterlagen auf andere Weise von den Tatorten entfernt wurden.

Den geschilderten Vorfall habe ich zum Anlass genommen, um noch einmal einen Ortstermin bei dem Unternehmen zu machen und mir die thematisierten Verfahren genauer schildern zu lassen. Zugleich war es meine zentrale Vorgabe, dass die Ablage der Protokolle künftig so gehandhabt wird, dass auch im Falle eines meldepflichtigen Vorkommnisses nach § 42a BDSG zeitnah und ohne weiteren Arbeitsaufwand zurückverfolgt werden kann, welcher Mitarbeiter für ein bestimmtes Krankenhaus zuständig ist und welche Patienten mithin seinem Zuständigkeitsbereich unterliegen.

Das mir vorgestellte Ablagesystem erfüllt meines Erachtens diese Kriterien. Im Ergebnis ist es damit jetzt möglich, konkret herauszufiltern, welcher Mitarbeiter welche Protokolle angefertigt hat. Ebenso kann zielgerichtet nach bestimmten Krankenhäusern gesucht werden. In der Datenbank befinden sich jedoch nicht die Protokolle selbst, diese werden separat abgelegt und nicht eingescannt. Faktisch ist es jedoch mit diesem Ablagesystem möglich, im Fall eines erneuten § 42a-Vorfalls zielgerichtet nach Dokumenten zu einem Mitarbeiter oder einem Krankenhaus zu suchen. Damit sind die diesbezüglich seitens des HDSB gemachten Vorgaben erfüllt.

Bei dem Gespräch wurde mir im Übrigen noch einmal mitgeteilt, dass auch die Dienstanweisung für die Außendienstmitarbeiter neu erstellt wurde und mithin deutlicher als bisher auf den korrekten Umgang mit den Protokollen hingewiesen wird. Für die Zukunft plane man im Übrigen, noch einmal auf den Prüfstand zu stellen, welche Angaben aus den Implantationsprotokollen man tatsächlich benötige. Insoweit wolle man auch noch einmal ein besonderes Augenmerk auf den Grundsatz der Datensparsamkeit richten. Sofern dies die Mitarbeiterin betrifft, die die Protokolle im Hausmüll entsorgt hat, habe man bereits mehrere Gespräche mit dieser geführt und diese nunmehr ihre Tätigkeit wieder aufnehmen lassen.

Bei dem Ortstermin habe ich mir auch noch einmal genauer erläutern lassen, weshalb die Anwesenheit von Mitarbeitern des Medizinprodukteherstellers bei einer Operation erforderlich ist. Wie mir dazu mitgeteilt wurde, erfolge die Anwesenheit oftmals auf Wunsch des Krankenhauses. Den Mitarbeitern kommt insoweit die Aufgabe zu, die eingesetzten Geräte noch einmal vor Ort zu kontrollieren und einzustellen. Es wurde jedoch auch noch einmal ganz klar festgehalten, dass die Verantwortung für die Dokumentation beim jeweiligen Krankenhaus liege. Die Protokolle haben insoweit weniger eine Bedeutung für etwaige Haftungsfälle, sondern vielmehr für die Rechnungsstellung sowie für die eigentlichen Kontroll- und Qualitätszwecke.

6.4

Einsatz von Patientenfragebogen im Bereich der medizinischen Fußpflege

Medizinisch notwendige Informationen können bereits vor Behandlungsbeginn vom Patienten eingeholt werden, wenn hierbei bestimmte datenschutzrechtliche Grundsätze beachtet werden.

6.4.1

Anlass

Ein Beschwerdeführer informierte mich darüber, dass er sich zu einem Behandlungstermin bei der in seiner Nähe gelegenen Fußpflege begeben habe. Bereits vor der Behandlung seien ihm ein die Schweigepflicht betreffendes Einwilligungsformular sowie ein Anamnesebogen vorgelegt worden. Darin wurde im Kontext mit der Fußpflege unter anderem abgefragt, wann sein letzter Zahnarztbesuch stattgefunden habe, welche Medikamente eingenommen würden und welche Vorerkrankungen bestünden. Ferner war auch die Schweigepflichtentbindung pauschal gehalten. So war darin unter anderem geregelt, dass der Therapeut der Praxis „jederzeit“ während der laufenden Behandlung den behandelnden Arzt konsultieren könne und „bei Notwendigkeit“ der Therapeut von seiner Schweigepflicht entbunden sei.

Auf meine Anfrage erläuterte mir die verantwortliche Stelle im Detail, wofür die einzelnen, im Anamnesebogen abgefragten Informationen erforderlich seien. Zugleich sagte mir die verantwortliche Stelle zu, künftig nur noch Formulare und Vordrucke eines Anbieters aus dem Raum Schleswig-Holstein zu verwenden. Ich habe daraufhin auch die neuen Formulare einer gesonderten Prüfung unterzogen. Hierbei wurden meine Kollegen aus Schleswig-Holstein mit einbezogen, die für den in Schleswig-Holstein ansässigen Anbieter der Formulare zuständig sind. Auch die neuen Formulare ließen aus meiner Sicht jedoch nicht hinreichend erkennen, wofür die erhobenen Daten erforderlich sind.

6.4.2

Rechtliche Bewertung

Auch im Bereich der Fußpflege gibt es selbstverständlich Informationen, die für den Behandler vorab von Interesse sein können und auch wichtig für die Behandlung sind. Dies betrifft sicherlich Hauterkrankungen, Gefäßerkrankungen oder Ähnliches. Dennoch kommt es häufig vor, dass durch derartige Fragenkataloge Daten abgefragt werden, die im Einzelfall für den jeweiligen Patienten oder Behandlungsanlass ohne Bedeutung sind. Hinzuweisen ist insoweit auf § 28 Abs. 7 BDSG, wonach Angaben über die Gesundheit nur erhoben werden dürfen, soweit dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung, der Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist. Ich vertrete die Auffassung, dass dem Behandelnden hierbei durchaus ein weiter Beurteilungsspielraum zusteht, welche Fragen er für erforderlich hält. Dem Patienten muss jedoch immer nachvollziehbar und verständlich sein, wieso einzelne Fragen gestellt werden. So war beispielsweise dem Beschwerdeführer nicht verständlich, weshalb nach seinem letzten Zahnarztbesuch gefragt wurde. Dies erschließt sich der Fachkraft unter Umständen ohne weiteres, dem Laien muss dies jedoch erst erläutert werden. Vor diesem Hintergrund habe ich dem Anbieter der Anamnesebogen einvernehmlich mit meinen Kollegen aus Schleswig-Holstein aufgegeben, eine Überarbeitung des Anamnesebogens dahingehend vorzunehmen, dass dem Patienten mit einem einleitenden Satz erklärt wird, wofür die Informationen benötigt werden und dass er, sofern ihm einzelne Fragen nicht verständlich sind, vor der Beantwortung vom Behandler eine ausführliche Erläuterung erhalten kann. Der Fragenkatalog konnte dann auch im Wesentlichen so bestehen bleiben.

Soweit dies die Entbindung von der Schweigepflicht gegenüber dem behandelnden Arzt betrifft, habe ich darauf bestanden, dass der Therapeut nicht jederzeit während der laufenden Behandlung den behandelnden Arzt konsultieren kann. Dies hat in jedem Fall erst nach vorheriger Rücksprache und Zustimmung seitens des Patienten zu erfolgen. Auch die Aussage, dass der Therapeut bei „Notwendigkeit“ von seiner Schweigepflicht entbunden wird, kann so nicht im Text bestehen bleiben.

6.4.3

Weitere Entwicklungen

Das in Schleswig-Holstein ansässige Unternehmen hat mittlerweile zugesagt, sämtliche verwendete Muster noch einmal hinsichtlich der genannten Aspekte zu überprüfen. Hiervon umfasst sind neben den Podologen auch andere Berufsgruppen wie Physiotherapeuten, Ergotherapeuten und Logopäden.

6.5

Auslagerung von IT-Dienstleistungen durch die AOK

Hinsichtlich einer geplanten Auslagerung von IT-Dienstleistungen durch die AOK Hessen wurde ich im vergangenen Jahr auch beratend tätig. Im Folgenden sollen einige technische und rechtliche Aspekte zu dem – soweit ersichtlich – bundesweit einzigartigen Projekt beleuchtet werden.

6.5.1

Sachverhalt und Fragestellungen

Bei dem IT-Dienstleister, der mich bezüglich des Projektes kontaktiert hat, handelt es sich um eine Arbeitsgemeinschaft der AOK Baden-Württemberg, der AOK Hessen und der AOK Rheinland-Pfalz, die in der Rechtsform einer GbR betrieben wird. Deren Aufgabe besteht in der Zurverfügungstellung und Optimierung gemeinsamer Bereiche der Informationstechnologie (IT) im Umfeld der Verarbeitung von Sozialdaten ausschließlich für die Gesellschafter. Zum Zwecke der Gewährleistung eines entsprechenden Standes der Technik und der Kostenminimierung beabsichtigt der Dienstleister – in diesem Fall als Auftraggeber –, den Rechenzentrumsbetrieb einschließlich weiterer Infrastrukturdienstleistungen auszulagern und künftig durch einen weiteren, privaten Sub-Dienstleister erbringen zu lassen. Hierfür vorgesehen ist ein sogenanntes Housing/Hosting-

Modell, bei dem der beauftragte Sub-Dienstleister tatsächlich keinen Zugriff auf die zentralen Datenspeicher des Auftraggebers haben soll. Der Auftraggeber hat sich deshalb dazu entschlossen, die Speichersysteme der Datenbanken und alle Dateisysteme, auf denen potentiell Sozialdaten gespeichert sein könnten, in einem Cage abzulegen. Unterstützt durch geeignete technische und organisatorische Maßnahmen sollen diese dort dem Zugriff durch den Sub-Dienstleister entzogen sein. Im Mittelpunkt der ausgelagerten Tätigkeit stehen mithin der Betrieb und die Wartung der zentralen Rechenzentrums-Infrastruktur. Hinzu kommen die Beschaffung, der Betrieb und die Wartung von Hard- und Software, aber ohne Speichersysteme.

Den Schwerpunkt der Prüfung in meinem Haus bildeten zunächst die Fragen zu den technisch-organisatorischen Maßnahmen im Hinblick auf die Projektziele. Zugleich war es aus rechtlicher Sicht eine zentrale Vorgabe, dass mittels der gewählten Lösung auch die Vorgaben des § 80 Abs. 5 SGB X eingehalten werden können.

§ 80 Abs. 5 SGB X

Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn

1. beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können oder
2. die übertragenen Arbeiten beim Auftragnehmer erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber oder beim Auftragnehmer, der eine öffentliche Stelle ist, und die Daten zur weiteren Datenverarbeitung im Auftrag an nicht-öffentliche Auftragnehmer weitergibt, verbleiben.

Gemäß dieser Vorschrift hat im Hinblick auf die gespeicherten Sozialdaten der überwiegende Teil der Speicherung des gesamten Datenbestandes beim Auftraggeber zu verbleiben.

Da im gegebenen Fall auch die Zuständigkeit meiner Kollegen aus Rheinland-Pfalz und Baden-Württemberg gegeben ist, habe ich mich mit diesen zu den zentralen Fragen abgestimmt. Im Rahmen des Projekts wurde ich immer wieder über den Stand der Ausschreibung informiert. Zugleich habe ich den Stand der Umsetzung bei einem Ortstermin im November 2016 in Augenschein genommen.

6.5.2
Lösungsansätze und Ausblick

Im Hinblick auf die Vereinbarkeit der geplanten Auftragsdatenverarbeitung mit den Vorgaben des § 80 Abs. 5 Nr. 2 SGB X hat der Dienstleister der AOK mehrere Rechtsgutachten eingeholt. Wie diese Gutachten und die in entsprechenden Unterlagen beschriebenen Ansätze zur technischen Umsetzung der Anforderungen komme auch ich zu dem Ergebnis, dass die Umsetzung des geplanten Projektes im Einklang mit den Vorgaben des § 80 Abs. 5 Nr. 2 SGB X möglich ist. Ein wesentliches Element ist hierbei ein Verschlüsselungskonzept. Danach werden die Sozialdaten verschlüsselt gespeichert. Dies gilt gleichermaßen für das Backup. Darüber hinaus erfolgt auch die Kommunikation verschlüsselt. Alle in diesem Kontext stattfindenden Prozesse unterliegen der vollständigen Administration durch den primären Dienstleister der AOK.

Auch im nächsten Jahr werde ich das Projekt weiter begleiten, um sicherzustellen, dass das Projekt tatsächlich im Einklang mit den datenschutzrechtlichen Vorgaben umgesetzt wird.

6.6
Prüfung von Krankenhausabrechnungen durch die KV Hessen

Im vergangenen Jahr hat die KV Hessen in meinem Zuständigkeitsbereich bei einigen Krankenhäusern Stichprobenprüfungen zum Zwecke der Kostenkontrolle gemäß § 106a Abs. 6 Satz 1 SGB V in Verbindung mit den hierzu ergangenen Richtlinien durchgeführt. Die Anschreiben an die Krankenhäuser waren jedoch derart unbestimmt, dass ich auf eine Überarbeitung hingewirkt habe.

6.6.1
Sachverhalt

Über das durchgeführte Verfahren der KV Hessen wurde ich erstmalig seitens der Datenschutzbeauftragten eines Krankenhauses informiert. Diese teilte mir mit, dass ihr Haus entsprechend angeschrieben worden sei und sich auch bereits ein Rundschreiben der Hessischen Krankenhausgesellschaft mit der Angelegenheit befasst habe. Darin wurden noch einmal die gesetzlichen Grundlagen für entsprechende Stichprobenprüfungen dargelegt. Seitens der Datenschutzbeauftragten wurde jedoch thematisiert, dass es nicht nachvollziehbar sei, welche Unterlagen genau für die Prüfung herauszugeben seien. In der Tat enthielt das Anschreiben bezüglich einiger ausgewählter Patienten, die sich in den Quartalen III/2014 bis II/2015 Notfallbehandlungen unterzogen haben, lediglich die Aussage, dass die „Patientenunterlagen zu den in der Anlage aufgelisteten Patienten“ bis zu einem bestimmten Stichtag zu übersenden sind. Hier war mithin völlig unklar, welche „Unterlagen“ aus der Behandlung tatsächlich für die Stichprobenprüfung benötigt werden.

Ich habe daraufhin mit der Datenschutzbeauftragten der KV Hessen Kontakt aufgenommen und um eine Abklärung mit dem zuständigen Fachbereich gebeten. Wie mir letztlich mitgeteilt wurde, waren von der Stichprobenprüfung 63 Krankenhäuser betroffen. Die Anzahl der zu übersendenden Unterlagen schwankte dabei zwischen einem und 152 Patienten je Klinik. Zugleich erfolgte der Hinweis, dass die bereits übersandten Unterlagen ganz unterschiedlicher Natur sind. So befanden sich darunter Dokumente wie Arztbriefe, Screenshots aus der Praxis-EDV mit den entsprechenden Aufzeichnungen zum Patienten, Röntgenbilder auf CD-ROM, Sonographie-Bilder und Messprotokolle sowie handschriftliche Aufzeichnungen. Diese Aussagen haben meinen Verdacht bestätigt, dass das Anschreiben der KV Hessen derart unbestimmt ist, dass die angeschriebenen Stellen tatsächlich nicht klar definieren können, welche Unterlagen sie herausgeben sollen.

6.6.2
Unsere Forderungen/ getroffene Maßnahmen

Bei der geschilderten Konstellation muss zunächst vorangestellt werden, dass auch die angeschriebene und abgebende Stelle ganz genau prüfen muss, welche Unterlagen zur Aufgabenerledigung tatsächlich benötigt werden. Es sind mithin von den Krankenhäusern nur die erforderlichen Aktenbestandteile an die KV Hessen weiterzuleiten. Eine entsprechende Bewertung war jedoch aufgrund der gegebenen Sachlage für die Krankenhäuser aus meiner Sicht nicht möglich. Ich habe daher zeitnah darauf hingewirkt, dass das Anschreiben an die Krankenhäuser entsprechend überarbeitet und genauer gefasst wird. Insbesondere war darin auch festzuhalten, welche Unterlagen nicht benötigt werden. Das überarbeitete Anschreiben enthielt nunmehr die folgende Information:

> „Inhalt der vorliegenden Stichprobe sind Notfallbehandlungen für die Quartale III/2014 bis II/2015, bei denen besonders behandlungsaufwendige Patienten aufgefallen sind. Um den gesetzgeberischen Auftrag erfüllen zu können, bitten wir Sie, uns die Unterlagen in Kopie zu den genannten Behandlungen zu den in der Anlage aufgeführten Patienten, unter Berücksichtigung der Behandlungstage, zu übermitteln. Die Unterlagen sollen Informationen über den Grund/die Ursache der Vorstellung enthalten. Reichen Sie uns hierzu, sofern vorhanden, den Aufnahme- bzw. Anamnesebogen ein. Nicht benötigt werden Bilder der diagnostischen und interventionellen Radiologie, CT, MRT und Ultraschalldiagnostik.“

Das entsprechend überarbeitete Schreiben wurde mittlerweile auch an die 63 betroffenen Krankenhäuser übersandt.

Nach meinen Informationen führte die KV Hessen erstmalig ein derartiges Verfahren in meinem Zuständigkeitsbereich durch. Ich habe daher darum gebeten, dass man nach Abschluss der Prüfung noch einmal intern bewertet, inwiefern das Schreiben für die Zukunft noch weiter modifiziert und genauer gefasst werden kann.

6.7
Lagerung von Patientenakten in einem Treppenhaus der Universitätsklinikum Gießen und Marburg GmbH (Standort Gießen)

Auch im vergangenen Jahr gab es wieder Datenschutzverstöße aus dem Gesundheitsbereich, die Gegenstand von Pressemeldungen waren. Erstaunlicherweise sind hiervon auch immer wieder Einrichtungen betroffen, bei denen man aufgrund deren Größe und Erfahrung im Gesundheitssektor eigentlich nicht davon ausgehen dürfte. Im Folgenden soll daher noch einmal der Fall betreffend das Universitätsklinikum Gießen und Marburg erörtert werden.

Im August 2016 informierte mich die Geschäftsführung der Universitätsklinikum Gießen und Marburg GmbH (UKGM), dass aufgrund eines „wahrscheinlich individuellen Fehlers“ Patientenakten im Bereich des Kinderherzzentrums Gießen für einen unbestimmten Zeitraum dem Zugriff Dritter ausgesetzt waren. Wie mir ferner mitgeteilt wurde, seien hierbei vermutlich auch zwei Patientenakten durch eine unbekannte Person entfernt und der Presse angeboten worden. Die lokale Presse habe es jedoch abgelehnt, diese anzunehmen. Schließlich wurde ich unterrichtet, dass man nach Bekanntwerden dieses Vorfalles die noch offen zugänglich gelagerten Akten unverzüglich der sicheren Aufbewahrung im Archiv zugeführt habe. Diese Ausführungen zu dem Ereignis wurden kurze Zeit später durch eine Pressemeldung bestätigt. Darin teilte der Informant noch einmal mit, dass in einem Treppenhaus des UKGM wochenlang dutzende Umzugskartons voller Patientenakten für jedermann zugänglich waren. Bei einem Besuch des Kinderherzzentrums habe er die Akten im Kellergeschoss unter einem Treppenabsatz gefunden. Der Informant war zunächst davon ausgegangen, dass die ca. 40 Kartons Akten eines Umzug beinhalten. Nachdem er diese auch noch nach zwei Wochen an der gleichen Stelle vorfand, habe er zwei der Akten entwendet, um diese der lokalen Presse anzubieten.

Aufgrund dieser Schilderung führte ich zeitnah Kontrollmaßnahmen vor Ort durch und informierte mich über die Hintergründe zu dem Sachverhalt. Bei dem Besuch des UKGM, der einige Tage später stattfand, habe ich mir neben der Station des Kinderherzzentrums auch noch einmal die Archivräume genauer angesehen.

Wie mir bei dem gemeinsamen Gespräch mit der Geschäftsführung, dem Leiter Compliance, dem Stationsarzt der Kinderkardiologie sowie Vertretern des Datenschutzes und der Rechtsabteilung mitgeteilt wurde, stammen die im Kellerflur gefundenen Patientenunterlagen aus einem Umzug, im Rahmen dessen sie verpackt, dort deponiert und vergessen wurden. Die Aufbewahrung sei zu „Studienzwecken“ erfolgt.

Soweit die Geschäftsführung immer wieder darauf hinwies, dass Besucher an der entsprechenden Stelle „nichts zu suchen haben“ und auch der Informant sich nicht korrekt verhalten habe, hat sie verkannt, dass das UKGM selbst dafür verantwortlich ist, dass kein Unbefugter Zugriff auf die Patientenakten nehmen kann. Erschwerend kommt hier hinzu, dass die Kartons nicht einmal auf der Station gelagert wurden, wo sie gegebenenfalls durch Personal hätten beaufsichtigt werden können. Vielmehr wurden sie in unbeaufsichtigten, allgemein zugänglichen Vorräumen zu den Behandlungsbereichen aufbewahrt (offenes Treppenhaus).

Bei dem Gespräch vor Ort teilte mir der stellvertretende Datenschutzbeauftragte noch einmal mit, welche Maßnahmen man künftig im Hause zur Vermeidung entsprechender Situationen durchführen wolle. Es handele sich hierbei um regelmäßige Informationen an die Mitarbeiter, Belehrungen, Pflichtfortbildung, Erstellung von Arbeitsanweisung zum Umgang mit Patientenakten sowie Begehungen.

Die aktuelle Arbeitsanweisung zum Umgang mit Patientenakten war zum Zeitpunkt meines Besuchs nur für das Pflegepersonal ausgestaltet. Die Arbeitsanweisung wurde im Nachgang mit meiner Unterstützung so erweitert und verändert, dass sie für das gesamte Klinikpersonal anwendbar ist. Die Arbeitsanweisung „Datenschutz – Patientenakte“ wurde mittlerweile auch an alle Mitarbeiter des Hauses versandt.

Im Folgenden hat mein Haus auch noch einmal Kontakt mit der Presse aufgenommen, um abzuklären, inwieweit der Informant dazu bewegt werden kann, die zwei entwendeten Akten wieder an das UKGM zurückzugeben. Erfreulicherweise konnte dies auf mein Betreiben hin auch erwirkt werden.

Zugleich habe ich bei meinem Besuch festgestellt, dass die laufenden Akten – so wie die zu archivierenden Akten aus dem Bereich der Kinderkardiologie – derzeit ordnungsgemäß verwahrt sind. Die Suche nach der innerhalb des UKGM für den Vorfall verantwortlichen Person ist nach meinen Informationen bislang erfolglos verlaufen.

Wie mir im Übrigen noch einmal versichert wurde, wurden die Akten nicht, wie anfänglich im Raum stand, für „Studienzwecke“ aufbewahrt. Dies wäre hier insoweit noch erschwerend zu berücksichtigen gewesen, da in diesen Fällen auch die Einwilligung der betroffenen Personen bzw. der Erziehungsberechtigten einzuholen gewesen wäre. Dies ist im Hinblick auf das Anfertigen der regulären Dokumentation zu Behandlungszwecken nicht der Fall, da § 630f BGB dies so zwingend vorsieht. Wie mir in diesem Kontext mitgeteilt wurde, habe es sich zum Zeitpunkt der Gründung des Fachbereichs an dem UKGM bei der Kinderkardiologie um ein relativ neues Fachgebiet gehandelt, bei dem keinerlei Vorerfahrung bestand. Vor diesem Hintergrund hatte man sich für eine Aufbewahrung von 30 Jahren entschieden, um gegebenenfalls gesundheitliche Nebenwirkungen/Langzeiteffekte besser beurteilen zu können. Eine klassische Auswertung zu Studienzwecken war jedoch zu keinem Zeitpunkt geplant. Der Hintergrund der längeren Aufbewahrung war es lediglich, Zusammenhänge zwischen aktuellen und potentiellen Erkrankungen der Patienten sowie eventuellen Folgen von der OP und/oder der Medikamentierung zu erkennen (Niereninsuffizienz etc.).

Seit einigen Jahren ist das Klinikum dazu übergegangen, die ärztliche Dokumentation ausschließlich elektronisch zu erfassen. Die Gefahr, dass bei einem erneuten Umzug einer Fachabteilung Vergleichbares passiert, ist dadurch zusätzlich reduziert.

6.8

Fehlende Zugangskontrolle in der Geschäftsstelle Frankfurt-Rödelheim des MDK Hessen

Im Rahmen einer Eingabe wurde mir mitgeteilt, dass es ohne Probleme möglich sei, als Besucher der MDK-Geschäftsstelle in Frankfurt-Rödelheim Bereiche zu betreten, in denen *sensible Patientendaten aufbewahrt werden. Während einer Prüfung und Begehung vor Ort musste ich feststellen, dass die Vorwürfe zutreffen. In Abstimmung mit dem Datenschutzbeauftragten des MDK Hessen habe ich daher den Einbau von Zugangssicherungen gefordert.*

Der Medizinische Dienst der Krankenversicherung (MDK) ist als medizinischer Beratungs- und Begutachtungsdienst für die gesetzlichen Kranken- und Pflegeversicherungen tätig. Ein Patient, der in der Geschäftsstelle des MDK Hessen in Frankfurt-Rödelheim lediglich ein Gutachten abholen wollte, schilderte mir, dass er hierbei ungehindert Räumlichkeiten betreten konnte, in denen sensible Patientendaten aufbewahrt werden. Sinngemäß wurde mir mitgeteilt, beim MDK Hessen habe es einen „Tag der offenen Tür“ gegeben. Der Hintergrund hierfür war offenbar der, dass sich sämtliche Mitarbeiter des Fachbereichs jeweils an dem besagten Wochentag zu einer gemeinsamen Sitzung treffen. Außerhalb der Öffnungszeiten ist die Geschäftsstelle zwar nicht zugänglich, jedoch war es dem Eingebenden möglich, die Gebäudeetage zu betreten, als ein Mitarbeiter der Geschäftsstelle diese zur Mittagspause verließ.

Da sich infolge der angesetzten Besprechung kein Mitarbeiter dieses Bereiches an seinem Arbeitsplatz befand, begab sich der Eingebende auf die Suche und konnte die internen Bereiche und die darin vorhandenen Einzelbüros betreten. Durch die räumliche Ausgestaltung der Büroetage war es ihm auch möglich, andere Arbeitsbereiche aufzusuchen. Zwar sind die Türen nur durch die Mitarbeiter mittels eines Chipkartenmechanismus zu öffnen, aus Brandschutzgründen konnten die Türen aber auch von jedermann ohne größere Schwierigkeiten manuell geöffnet werden, so auch vom Eingebenden.

In den auf diese Weise betretenen Bereichen befand sich neben einem unverschlossenen Aktenschrank mit medizinischen Unterlagen von Patienten auch ein offener Postschrank.

Nachdem der Eingebende schließlich einen Mitarbeiter aus einem anderen Bereich der Geschäftsstelle angesprochen hatte, wurde er in den Besprechungsraum geführt und erhielt von dort aus sein Gutachten.

Kurze Zeit später wandte sich der Eingebende an den Datenschutzbeauftragten des MDK-Hessen. Dieser bat die verantwortlichen Personen der MDK-Geschäftsstelle in Frankfurt-Rödelheim zwar um Stellungnahme, eine örtliche Begehung erfolgte jedoch nicht. Als Rückmeldung erhielt der Eingebende lediglich die Information, dass man die Mitarbeiter angesichts der Hinweise bezüglich des Datenschutzes und der Datensicherheit im Umgang mit Sozialdaten sensibilisiert habe. Der Eingebende nahm daher noch einmal mit meinem Haus Kontakt auf.

Aufgrund der Eingabe habe ich mir zusammen mit dem Bereichsleiter der Geschäftsstelle, einer Mitarbeiterin der Verwaltung und dem Datenschutzbeauftragten die fraglichen Bereiche vor Ort angesehen und den Sachverhalt insgesamt erläutert.

Der MDK erklärte, dass die internen Bereiche der Geschäftsstelle gegenüber dem öffentlichen Bereich (dem Empfang, den Warte- und den Untersuchungszimmern) zwar durch Türen abgetrennt sind, diese aber aufgrund von Brandschutzanforderungen (Fluchttüren) nicht verschlossen werden dürfen. Außerdem ging man davon aus, dass ein jeweiliges Schild mit dem Aufdruck „Zutritt nur für Personal“ ausreichend sei, um sicherzustellen, dass kein Unbefugter sich Zutritt zu den nicht-öffentlichen Bereichen verschafft.

Zunächst muss vorangestellt werden, dass Maßnahmen gegen unbefugtes oder unbeaufsichtigtes Betreten eines Bereiches nur erfolgreich sind, wenn neben entsprechenden Zugangssicherungen von außen auch das Personal beim Betreten oder Verlassen des Bereiches darauf achtet, dass Dritte nicht über (noch) nicht geschlossene Türen die Räumlichkeiten betreten.

Weiterhin muss sichergestellt sein, dass – sofern eigenes Personal in einem öffentlichen Bereich vorübergehend nicht verfügbar ist – es den sich hier aufhaltenden Personen nicht möglich ist, Bereiche zu betreten, in denen sensible Daten aufbewahrt werden.

Wie mir im vorliegenden Fall mitgeteilt wurde, sind größere, bauliche Maßnahmen nicht bzw. nur mit erheblichem Aufwand leistbar, da zum einen die MDK-Geschäftsstelle nur Mieter der Büroetage ist und zum anderen brandschutztechnische Anforderungen einer permanenten Türsicherung entgegenstehen. Vom MDK wurde mir daher der Vorschlag unterbreitet, die Türen, die in die Bereiche führen, in denen sensible Daten aufbewahrt werden, mit einem elektronischen Türwächter auszustatten, der beim manuellen Öffnen der Tür ein Signal auslöst. Das Signal ist dabei entsprechend laut hörbar, so dass Mitarbeiter zeitnah darauf reagieren können.

Soweit dies den Übergang zu den anderen Bereichen der MDK-Geschäftsstelle betrifft, wird die dortige Tür künftig von der Seite, in der sich die Warteräume befinden, nicht mehr zu öffnen sein.

Die genannten baulichen Maßnahmen habe ich aus datenschutzrechtlicher Sicht als ausreichend erachtet. Des Weiteren wurden die Mitarbeiter noch einmal mittels eines Merkblattes über die zu ergreifenden Sicherheitsmaßnahmen bei der Übermittlung und Verarbeitung sensibler, personenbezogener Daten informiert.

Der Fall hat gezeigt, dass immer wieder daran erinnert werden muss, Akten – besonders im medizinischen Bereich – gegenüber unbefugten Dritten abzusichern, auch wenn diese sich in einem vermeintlich sicheren Bereich befinden. Zudem ist es ratsam, bei entsprechenden Meldungen als zuständiger Datenschutzbeauftragter selbst vor Ort eine Begehung durchzuführen, um die Gefahren für die Datensicherheit im Bereich der Zugangskontrolle genauer abschätzen zu können.

6.9

Prüfung des Krankengeldfallmanagements bei der AOK Hessen

In der Vergangenheit gab es bundesweit immer wieder Diskussionen bezüglich der Einhaltung der datenschutzrechtlichen Vorschriften im Zusammenhang mit dem von den gesetzlichen Krankenkassen durchgeführten Krankengeldfallmanagement. Ich habe dies zum Anlass genommen und im letzten Jahr eine stichprobenhafte Prüfung von Krankengeldfallakten bei der AOK Hessen durchgeführt.

Sachverhalt

Seit Jahren versuchen Krankenkassen, im Rahmen ihrer Möglichkeiten Langzeit-Arbeitsunfähige und Krankengeldbezieher speziell zu betreuen und zu unterstützen. Zu einer solchen Betreuung durch die Krankenkasse gehören beispielsweise persönliche Beratungen der Versicherten ebenso wie die Koordination zwischen den medizinischen Dienstleistungsangeboten und Unterstützung bei der Inanspruchnahme verschiedener Leistungen des Sozialversicherungssystems. Durch diese systematische Steuerung des Arbeitsunfähigkeitsfalles (Krankengeldfallmanagement) hofft die Krankenkasse, zu einer schnelleren Gesundung des Patienten und damit verbunden zu einer rascheren Wiedereingliederung in das Erwerbsleben beizutragen. Nicht zuletzt sollen auf diese Weise auch Krankengeldkosten eingespart werden. Wie einzelne Datenschutzaufsichtsbehörden dabei seit Jahren feststellten, kam es bei den Krankenkassen bei der Betreuung der arbeitsunfähigen Mitglieder nicht selten zu einem datenschutzrechtlich bedenklichen Umgang mit deren Sozialdaten. Die Krankenkassenmitarbeiter erhoben zum Teil umfangreiche detaillierte Gesundheitsdaten von Versicherten, die längere Zeit arbeitsunfähig waren oder bereits Krankengeld erhielten, ohne dass es eine ausreichende rechtliche Grundlage für die Erhebungen gab. Auch die vom Gesetzgeber vorgesehene Aufgabentrennung zwischen dem Medizinischen Dienst der Krankenversicherung (MDK) und den gesetzlichen Krankenversicherungen wurde von den Krankenkassen dabei oft nicht beachtet. So wurden beispielsweise bei der Anforderung von medizinischen Unterlagen für den MDK im sog. Umschlagverfahren, bei dem Vertragsärzte die Unterlagen über die Krankenkassen in einem verschlossenen Umschlag an den MDK weiterleiteten, in der Vergangenheit teilweise die Umschläge unzulässigerweise von den Krankenkassen geöffnet und von den Krankenkassenmitarbeitern zur Kenntnis genommen. Krankenkassen in meinem Zuständigkeitsbereich waren dabei bislang nicht auffällig. Ich habe die bundesweite Diskussion bezüglich des Krankengeldfallmanagements jedoch zum Anlass genommen, mir die Abläufe bei der größten hessischen Krankenkasse genauer anzusehen.

Rechtlicher Rahmen des Krankengeldfallmanagements

Der Gesetzgeber hat in den Sozialgesetzbüchern geregelt, unter welchen Voraussetzungen gesetzliche Krankenkassen Daten erheben dürfen. Nach § 284 SGB V sind Krankenkassen z. B. berechtigt, Sozialdaten für Zwecke der Krankenversicherung zu erheben und zu speichern, wenn dies für die Prüfung der Leistungspflicht und die Erbringung von Leistungen an Versicherte oder zur Einschaltung des MDK erforderlich sein sollte. Hierzu dürfen sie dann auch Kontakt mit den Versicherten aufnehmen, um bestimmte Informationen zu erfragen.

In der Vergangenheit wurden von den Datenschutzaufsichtsbehörden teilweise unterschiedliche Ansichten bezüglich der Zulässigkeit und der Reichweite der bisherigen Vorschriften mit Blick auf das Krankengeldfallmanagement vertreten. Durch das Gesetz zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz – GKV-VSG) vom 16.07.2015 (BGBl. I S. 1211) hat der Gesetzgeber reagiert und es wurde das SGB V um einen gesetzlichen Anspruch auf ein Krankengeldfallmanagement erweitert.

Nach § 44 Abs. IV SGB V haben Versicherte einen Anspruch auf individuelle Beratung und Hilfestellung durch die Krankenkasse, welche Leistungen und unterstützenden Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind. Die entsprechenden Maßnahmen durch die Krankenkasse und die dazu erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Daten dürfen jedoch nur mit schriftlicher Einwilligung und nach vorheriger schriftlicher Information des Versicherten erfolgen. Die Einwilligung in das Krankengeldfallmanagement muss auf freiwilliger Basis erfolgen, sie kann jederzeit schriftlich widerrufen werden und eine Ablehnung darf keine leistungsrechtlichen Konsequenzen für den Versicherten haben.

Die sich daraus ggf. ergebenden erweiterten Datenerhebungsmöglichkeiten im Rahmen der „individuellen Beratung und Hilfestellung“ durch die Krankenkassen bleiben jedoch – wie bislang auch – durch den gesetzlichen Aufgabenbereich des MDK in Fällen des § 275 SGB V begrenzt. Eine Erweiterung der Zuständigkeiten der Krankenkasse auf Aufgabenfelder des MDK hat der Gesetzgeber auch nicht durch die Neuregelungen des GKV-Versorgungsstärkungsgesetz vorgesehen. Durch die Ergänzung des § 44 SGB V um die individuelle Beratung und Hilfestellung durch die Krankenkasse im Krankheitsfall gibt es jetzt einen verbindlichen rechtlichen Rahmen für die Durchführung eines Krankengeldfallmanagements.

Prüfung bei der AOK Hessen

Im Frühjahr 2016 habe ich eine stichprobenhafte Prüfung der Einhaltung der datenschutzrechtlichen Vorschriften beim Krankengeldfallmanagement bei der AOK Hessen durchgeführt.

Die AOK hat bereits seit vielen Jahren ein Krankengeldfallmanagement etabliert. Spezielle Mitarbeiter übernehmen dabei die Betreuung der Arbeitsunfähigen bzw. Krankengeldbezieher. Je nach Diagnose oder sonstigen Umständen, z. B. Arbeitslosigkeit, Arbeitsunfähigkeit als Unfallfolge, entscheidet die Krankenkasse, ob Maßnahmen im Sinne eines Fallmanagements einzuleiten sind. Ziel ist es, mit dem Versicherten in Kontakt zu treten und wenn möglich ein persönliches Beratungsgespräch zu führen. Eine Betreuung im Rahmen eines Krankengeldfallmanagements erfolgt laut AOK Hessen grundsätzlich erst dann, wenn der Versicherte -wie gesetzlich vorgesehen- eine Einwilligungserklärung nach § 44 Abs. 4 SGB V unterzeichnet hat. In den Beratungsgesprächen mit den Versicherten werden dann deren individuelle Situation, die Bedürfnisse und die persönliche Zielsetzung der Versicherten erörtert. Gesprächsinhalte sind u. a. Informationen über die Krankengeldhöhe und den Krankengeldbeginn, die Zahlungsmodalitäten, die aktuelle und geplante Behandlungssituation, die Möglichkeiten der Unterstützung durch die Krankenkasse sowie Abstimmung mit dem Versicherten über den weiteren Verlauf. Dabei werden teilweise auch medizinische Daten erhoben bzw. vom Krankenkassenmitarbeiter zur Kenntnis genommen. Der überwiegende Teil der medizinischen Unterlagen werde von den Versicherten selbst beigebracht.

Soweit medizinische Unterlagen speziell für die Vorlage beim MDK bei Leistungserbringern (z. B. Ärzten) angefordert werden, erfolgte dies bislang über das sogenannte Umschlagverfahren, bei dem die Vertragsärzte die Unterlagen über die Krankenkassen in einem verschlossenen Umschlag an den MDK weiterleiteten.

Durch eine Neuregelung des § 276 Abs. 2 SGB V zum 01.01.2016 ist dieses bisher von mir tolerierte und von der AOK Hessen praktizierte Umschlagverfahren unzulässig geworden.

> § 276 Abs. 2 SGB V
>
> Der Medizinische Dienst darf Sozialdaten erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 erforderlich ist. Haben die Krankenkassen oder der Medizinische Dienst für eine gutachtliche Stellungnahme oder Prüfung nach § 275 Absatz 1 bis 3 erforderliche versichertenbezogene Daten bei den Leistungserbringern angefordert, so sind die Leistungserbringer verpflichtet, diese Daten unmittelbar an den Medizinischen Dienst zu übermitteln.

Die von Krankenkassen für den MDK angeforderten Unterlagen sind nun immer unmittelbar an den MDK zu übermitteln. Um dies technisch umzusetzen, haben die Krankenkassen und MDKs ein elektronisches Mitteilungs-/Datenaustauschverfahren eingerichtet, das nach Angabe der AOK Hessen ab 01.01.2017 in Betrieb geht.

Bei meinen stichprobenhaften Prüfungen der Fallakten konnte ich die von der AOK Hessen gemachten Angaben soweit nachvollziehen. Der Umfang der im Rahmen des Krankengeldfallmanagements erhobenen Daten war in den geprüften Akten plausibel und für mich nachvollziehbar. Die für das Krankengeldfallmanagement nach § 44 Abs. 4 SGB V notwendige schriftliche Einwilligungserklärung der Versicherten lag jeweils vor. Da die Erklärungen in der Regel im persönlichen Gespräch eingeholt werden, habe ich die AOK

Hessen darauf hingewiesen, dass ausdrücklich auf die Freiwilligkeit der Inanspruchnahme der Maßnahmen nach § 44 Abs. 4 SGB V hinzuweisen ist und auch im Beratungsgespräch kein Druck auf die Versicherten ausgeübt werden darf.

Teilweise waren den geprüften Krankengeldakten auch Daten von Angehörigen zu entnehmen. Auch wenn es vielleicht in manchen Fällen für die Fallbetreuung wichtig erscheint, ist darauf zu achten, dass in den Fallakten keine personenbezogenen Daten Dritter gespeichert werden. Generell dürfen nur die Daten erhoben/gespeichert werden, die für die Fallbearbeitung tatsächlich erforderlich sind. Dies ist auch dann zu beachten, wenn die Versicherten Unterlagen ohne Aufforderung von sich aus beibringen.

Insgesamt hat meine stichprobenhafte Prüfung der Krankengeldfallakten der AOK Hessen keine Anhaltspunkte für rechtswidrige Abläufe ergeben.

6.10
Unberechtigte Zugriffe auf Patientenakten nach Schießerei im Krankenhaus

Ein Fall unberechtigter interner Zugriffe auf Patientenakten zeigt erneut die Notwendigkeit eines angemessenen Rollen- und Berechtigungskonzepts für die Zugriffe auf das Krankenhausinformationssystem. Das Krankenhaus wird sein Rollen- und Berechtigungskonzept überarbeiten. Ich werde die Entwicklung des Konzepts beratend begleiten.

Im Juli 2016 erhielt meine Dienststelle Kenntnis davon, dass es in einer Klinik den Verdacht auf unberechtigte Zugriffe auf Patientenakten gab. Hintergrund war ein Zwischenfall auf einer Station, bei der ein Patient mit einer Pistole um sich geschossen und dabei mehrere Klinikmitarbeiter verletzt hatte. Da dieser besondere Vorfall von den Medien aufgegriffen wurde, veranlasste die Geschäftsführung vorsorglich eine Prüfung der erfolgten internen Zugriffe auf die elektronischen Patientenakten der betroffenen Klinikmitarbeiter. Von der IT-Abteilung wurden die Zugriffe auf die Patientenakten ermittelt und mit den Namen und Einsatzorten der jeweiligen Mitarbeiter des Klinikums verknüpft. Es wurden dann auf Basis eines Gesprächsleitfadens in Abstimmung mit dem Betriebsrat Gespräche mit den Mitarbeitern geführt, die im Verdacht standen, unberechtigt auf die Patientendaten zugegriffen zu haben.

Die klinikinterne Prüfung ist noch nicht abgeschlossen. Nach Mitteilung der Geschäftsführung stellte sich aber bereits heraus, dass eine Reihe von Mitarbeiterinnen und Mitarbeitern – sowohl ärztliches wie auch pflegerisches Personal – aus verschiedenen Abteilungen unberechtigt auf die Krankenakten der Krankenhausmitarbeiter zugegriffen bzw. nach deren Darstellung sich nicht ausgeloggt und dadurch einen unberechtigten Zugriff anderer ermöglicht haben. Dies lässt vermuten, dass das Rollen- und Berechtigungskonzept der Klinik zu diesem Zeitpunkt nicht, wie von meiner Dienststelle immer gefordert, hinreichend differenziert war. Die Geschäftsführung teilte mir Ende Oktober 2016 auch mit, dass als Reaktion auf den Vorfall und zur Verhinderung weiterer vergleichbarer Ereignisse die Umsetzung eines stringenteren Zugriffskonzepts als notwendig angesehen wird.

Zuletzt in meinem 44. Tätigkeitsbericht (Ziff. 4.8.6) berichtete ich bereits über einen ähnlichen Fall, bei dem Klinikmitarbeiter unberechtigt auf elektronische Patientenakten zugriffen. Seit dem Jahr 2011 gibt es als Reaktion auf bundesweit festgestellte Defizite bei Krankenhausinformationssystemen als Hilfestellung für die datenschutzgerechte Ausgestaltung von Krankenhausinformationssystemen die von den Datenschutzbeauftragten des Bundes und der Länder erstellte Orientierungshilfe für Krankenhausinformationssysteme (OH KIS, Version 2014 https://www.datenschutz.hessen.de/ft-gesundheit.htm). Ich habe mich in meinen letzten Tätigkeitsberichten immer wieder ausführlich mit dem Thema Rollen- und Berechtigungskonzepte für die Zugriffe auf Krankenhausinformationssysteme befasst. Patienten gehen nicht davon aus und müssen nicht davon ausgehen, dass die gesamte Belegschaft eines Krankenhauses ihre Krankheitsdaten zur Kenntnis nehmen kann. Das entsprechende Rollen- und Berechtigungskonzept und dessen Umsetzung haben sicherzustellen, dass Mitarbeiter im Klinikum nur Zugriff auf die Patientendaten haben, die sie tatsächlich für ihre Aufgabenerfüllung benötigen.

Allerdings muss ein Rollen- und Berechtigungskonzept für ein Krankenhaus wegen der komplexen Aufgaben noch ausreichend Flexibilität ermöglichen (z. B. für Notfälle, Überbelegung, Nachtdienst, Verlegung, Konsil). Die Protokollierung der Zugriffe im KIS und eine regelmäßige Auswertung der Protokolle auf der Grundlage eines schriftlich verbindlich festgelegten Konzepts ist in diesem Zusammenhang von zentraler Bedeutung für die datenschutzgerechte Ausgestaltung des KIS.

Positiv zu erwähnen ist im konkreten Fall, dass die Geschäftsleitung von sich aus eine Prüfung der erfolgten Zugriffe veranlasst hatte und sich damit der datenschutzrechtlichen Risiken wohl bewusst war. Ein datenschutzgerechtes Konzept muss auch ein angemessenes Protokollierungs- und Auswertungskonzept einschließen. Dazu gehört im

Rahmen der vorbeugenden Datenschutzkontrolle auch, Protokolle turnusmäßig auf bestimmte Auffälligkeiten hin, wie z. B. eine Häufung von Abfragen bestimmter Benutzerkennungen, eine Häufung von Abfragen außerhalb der Dienstzeiten oder unübliche Suchkriterien, auszuwerten.

Die Geschäftsleitung der Klinik hat zugesichert, noch im 1. Quartal 2017 stichprobenhafte Kontrollen der Zugriffe auf Krankenakten einschließlich einer Dokumentation der erfolgten Kontrollen und veranlassten Maßnahmen einzuführen und ab 2017 Einschränkungen des Zugriffskonzepts bzw. eine umfangreiche Anpassung des Rollen- und Berechtigungskonzepts vorzunehmen.

6.11

Einführung der digitalen Verarbeitung der Einsatzdaten in der Rettungsleitstelle Fulda

Die Einführung der digitalen Verarbeitung der Einsatzdaten in einer Rettungsleitstelle kann eine schnellere und sicherere Kommunikation zwischen den Beteiligten ermöglichen. Für die datenschutzgerechte Ausgestaltung des Verfahrens habe ich gegenüber den Projektverantwortlichen Anforderungen formuliert.

2015 entschied sich der Landkreis Fulda für die Einführung des digitalen Verfahrens NIDA. Das Projekt befindet sich noch in der Probephase. Da ich bereits diverse Anfragen zur Einführung einer digitalen Verarbeitung von Einsatzdaten in Rettungsleitstellen erhalten habe und in anderen Bundesländern eine digitale Verarbeitung zum Teil bereits flächendeckend eingeführt wurde, habe ich mich im Juni 2016 vor Ort über den Stand des Projekts in Fulda informiert und Fragen einer datenschutzgerechten Ausgestaltung dort besprochen.

6.11.1

Zentrale Aspekte der neuen Abläufe

Die bisherige Verfahrensweise in der Leitstelle war wie folgt:
Das Einsatzprotokoll mit den Abrechnungsdaten, Vitaldaten, Informationen über die Besatzung sowie evtl. weiteren medizinischen Daten (z. B. EKG), Bildern (z. B. von zerstörten Fahrzeugen) wird nach Abschluss des Einsatzes im Rettungsfahrzeug geschrieben und je ein Ausdruck dem aufnehmenden Krankenhaus, dem Notarzt und dem Rettungsdienst selbst zur Verfügung gestellt. Für die Voranmeldung des Patienten an den Krankenhäusern werden Daten zum Zustand des Patienten und zum Einsatz manuell vom Leitstellenmitarbeiter eingetragen und über IVENA an das Krankenhaus übermittelt.

Das neue Verfahren setzt auf stärker elektronisch unterstützte Abläufe. Daran sind folgende technische Komponenten beteiligt:

- ein Kommunikationsserver, das NIDA-Gateway,
- ein Anwendungsserver samt Datenspeicherung, den NIDA-Server,
- die Endgeräte in den Einsatzfahrzeugen, die PADs, und
- Programme für den Zugriff auf die Daten von PCs aus, der NIDA-Client.

Die beiden Server werden bei der ekom21 gehostet und durch den Anbieter der Lösung, die Firma medDV GmbH, administriert.

Die Abläufe sollen zukünftig wie folgt sein:

- Vorbereitend meldet bei Schichtbeginn die Besatzung eines Einsatzfahrzeuges sein PAD mit dem Funkrufnamen des Fahrzeugs und sich selbst mit ihren Benutzerkennungen am NIDA-Gateway an. Damit ist das PAD einsatzbereit und Gerät sowie Besatzung sind im System aktiv.

- Der Einsatz läuft in der Regel wie folgt ab:
    - Es erfolgt ein Telefonanruf in der Leitstelle.
    - Die Leitstelle erfasst die Daten elektronisch.
    - Die Leitstelle wählt mittels ihrer Software das passende Einsatzfahrzeug aus und alarmiert es.
    - Wenn das PAD des vorgesehenen Fahrzeugs angemeldet ist – was bei Schichtbeginn erfolgt –, wird es über das NIDA-Gateway unter dem Funkrufnamen mit den Einsatzdaten (Einsatznummer = Transportscheinnummer), Datum, Zeit, Adresse, evtl. Verdachtsdiagnose etc. versorgt. Das Gateway sendet Daten nur an das mit dem entsprechenden Funkrufnamen angemeldete PAD.
      Der Abruf von Daten wird vom PAD initiiert, das den Server regelmäßig anfragt, ob neue Daten vorhanden sind.
    - Der Empfang der Daten wird vom PAD des Einsatzfahrzeugs quittiert.
    - Der Notarzt wählt das Krankenhaus aus und er wählt die Einsatzdaten aus, die das Krankenhaus per Voranmeldung erhalten soll. Das kann auf drei Arten geschehen: per Protokoll als pdf-Datei, mit anonymisierten Daten oder es werden die Daten an Server in dem Krankenhaus übertragen.

Für den Zugriff auf die Daten benötigt man den NIDA-Client. Dieser Client wird von den Krankenhäusern gekauft. Der Administrator des Krankenhauses betreut den Client. Insoweit ist für den Notarzt die Verarbeitung der personenbezogenen Patientendaten transparent.

- Nach abgeschlossenem Einsatz (mit km-Stand, Uhrzeit) wird der Einsatz durch Knopfdruck auf dem PAD abgeschlossen. Es ist konfiguriert, welche Stelle welche Daten erhält, z. B. die Feuerwehr erhält die Abrechnungsdaten.

- Daten zu einem Einsatz (Einsatzprotokoll als pdf-Dokument und evtl. Bilder) werden an den NIDA-Server übertragen und bleiben dort gespeichert. Das Protokoll ist so aufgebaut, dass die verschiedenen Stellen/Personen mit Zugriffsrechten jeweils Zugriff auf den Teil haben, der für sie relevant ist. Die diesbezüglichen Regeln werden in einem Datenschutz- und Datensicherheitskonzept beschrieben, das auf Grundlage des Gesprächs noch angepasst wird. Es wird mir in der dann aktuellen Fassung zur Verfügung gestellt.

- Da die Leitstelle keinen Zugriff auf den NIDA-Server hat, wird das Einsatzprotokoll automatisch an sie weitergeleitet.

- Die Einsatzdaten werden nach erfolgreicher Übertragung an den NIDA-Server auf dem PAD gelöscht. Sollte die Übertragung nicht möglich sein, beispielsweise wegen schlechter Netzverbindung, so können die Daten von bis zu fünf Einsätzen gespeichert sein.

6.11.2
Datenschutzrechtliche Aspekte des Projekts

Zur datenschutzgerechten Ausgestaltung des Projekts habe ich noch einige Konkretisierungen bzw. Änderungen gefordert:

- Für den Abruf der Daten/Bilder vom NIDA-Server muss es ein Konzept geben, das nach Rollen (z. B. Rettungsdienstmitarbeiter, Besatzung des Rettungsmittels, Mitarbeiter einer benannten Wache, Administratoren usw.) und Berechtigungen (z. B. Zugriff nur auf Stammdaten, Zugriff auf alle Patienten- und Personaldaten nur im Einzelfall mit Begründung, Zugriff auf alle Patienten- und Personaldaten ohne Begründung usw.) differenziert. Das Konzept wird gegenwärtig überarbeitet und ist noch Gegenstand der Diskussion.
  In jedem Fall dürfen die eingesetzten Rettungskräfte und Notärzte mit ihrer Benutzerkennung (nur) alle Daten ihrer eigenen Einsätze einsehen.

- Klärungsbedürftig ist noch, wer die Befugnis hat, Rollen/Rechte für den Zugriff auf den Server eintragen zu lassen und wer die Einträge vornimmt und dokumentiert.

- Hinsichtlich der getroffenen Datensicherheitsmaßnahmen habe ich gefordert, dass das Datenschutz- und Datensicherheitskonzept noch einmal überarbeitet wird. Das betrifft u. a. den Zugriff auf den NIDA-Server über das Internet. Eine Überarbeitung wurde bereits zugesagt.

6.12
Schutz gegen unberechtigte Zugriffe bei der Verwendung mobiler Arbeitsstationen in Krankenhäusern

Im Rahmen einer Beschwerde über ein Krankenhaus wurden mir Bildschirmfotos von einem Krankenhausinformationssystem übermittelt, die von einer unbeaufsichtigten, im Krankenzimmer befindlichen mobilen Arbeitsstation stammen. Im Rahmen einer unangekündigten Prüfung habe ich den Vorfall mit Verantwortlichen erörtert und mir die Arbeitsumgebung auf einer Station des Klinikums angesehen. Die gegen das Klinikum erhobenen Vorwürfe waren zutreffend, eine umgehende Anpassung der Systemkonfiguration wurde veranlasst.

Im Rahmen einer Beschwerde über einen ungesicherten Zugang zum Krankenhausinformationssystem eines Klinikums wurden mir zur Untermauerung der Vorwürfe Bildschirmfotos einer mobilen Arbeitsstation übermittelt, von der aus auf die elektronische Krankenakte zugegriffen wurde. Den Besuchern des Patienten war problemlos der Zugang zum System möglich, da lediglich der Monitor über die Energieverwaltung des Betriebssystems abgeschaltet war, jedoch war weder der Zugang zum Windows-Betriebssystem noch zum Krankenhausinformationssystem ausreichend abgesichert.

Die mobilen Arbeitsstationen werden sowohl mobil für die tägliche Arbeit als auch stationär bei besonderen Anforderungen (z. B. wenn das Gerät wegen besonderer Infektionsgefahr beim Patienten verbleiben muss) eingesetzt.

Bei mobil eingesetzten Geräten findet in aller Regel neben den Absicherungen des Betriebssystems und der Anwendungen zusätzlich eine „soziale Kontrolle“ statt (z. B. werden momentan nicht eingesetzte Geräte auf dem Flur abgestellt, so dass sofort auffällt, wenn nicht zur Station gehörende Personen daran arbeiten). Stationäre Geräte bedürfen hingegen einer erweiterten Absicherung, da in aller Regel auch die Zimmertüren geschlossen sind und damit nicht unmittelbar auffällt, wenn sich nicht zum Krankenhauspersonal gehörige Personen Zugang zum Gerät verschaffen.

Auch muss berücksichtigt werden, dass eventuell Personal, das am Gerät arbeitet, in Folge eines Notfalls plötzlich (und dringend) zu einem anderen Patienten muss.

Damit stehen den Anforderungen des Datenschutzes – die zudem im Bereich der medizinischen Daten noch höher als üblich sind – die Anforderungen des Klinikpersonals an eine nutzbare Arbeitsumgebung entgegen.

Dieses Argument kann aber nicht als Begründung – zudem entgegen den Einlassungen des betrieblichen Datenschutzbeauftragten – für das Fehlen eines Bildschirmschoners dienen. Als „Absicherung“ gegen unberechtigte Zugriffe lediglich den Monitor über die Energieverwaltung des Betriebssystems abzuschalten, reicht nicht aus.

Für solche Systeme ist es zwingend erforderlich, in enger Abstimmung zwischen Personal, IT-Administration und dem Datenschutzbeauftragten eine sowohl den Anforderungen des Datenschutzes als auch dem praktikablen Arbeiten gerechte Lösung zu finden.

Zwischenzeitlich sind auch Anwendungen am Markt verfügbar, die in der Lage sind, das Betriebssystem zu sperren, wenn ein definiertes Gerät (Chipkarte, USB-Stick, Bluetooth- oder NFC-fähiges Gerät) nicht mehr an die Arbeitsstation angeschlossen ist bzw. sich nicht mehr in einem definierten Radius im Empfangsbereich der Arbeitsstation befindet.

6.13

Datenschutz im Verfahren zur Anerkennung der Beihilfefähigkeit einer psychotherapeutischen Behandlung

Sowohl im Antragsverfahren als auch im Genehmigungsverfahren für die Anerkennung der Beihilfefähigkeit einer psychotherapeutischen Behandlung sind die hierfür geltenden datenschutzrechtlichen Vorschriften unbedingt einzuhalten. Keinesfalls darf die Anerkennung des Verfahrens von einem Magistratsbeschluss abhängig gemacht werden.

Anlass

Anlass der Befassung mit diesem Thema war die Eingabe eines städtischen Bediensteten. Dieser hatte einen Antrag auf Anerkennung der Beihilfefähigkeit einer Psychotherapie zusammen mit dem Bericht seines behandelnden Therapeuten bei der Beihilfefestsetzungsstelle seiner Dienststelle eingereicht. Dieser zunächst formlos gestellte Antrag war von der Dienststelle an den Auftragsdatenverarbeiter für Beihilfeangelegenheiten zur weiteren Bearbeitung gesandt worden. Von dort wurde der Antrag umgehend an die Dienststelle zurückgereicht mit dem Hinweis, es müsse zunächst ein Gutachterverfahren durchgeführt werden und über die Beihilfefähigkeit der Maßnahme entschieden werden. Ein (veraltetes) Antragsformular war beigefügt. Daraufhin führte die Stadt einen Magistratsbeschluss herbei, „bewilligte“ den Antrag und leitete anschließend in einem förmlichen Antragsverfahren den Bericht des Therapeuten an zwei unabhängige Gutachter weiter. Der den Bericht enthaltende verschlossene Umschlag war inzwischen geöffnet worden, der Petent fühlte sich „einem Spießrutenlauf“ ausgesetzt und meinte, gemessen daran, wie viele Personen bereits Kenntnis von seiner geplanten Behandlung hätten, hätte er seinen Antrag auch gleich in der Presse veröffentlichen können.

Meine Nachfrage beim Bürgermeister der Stadt ergab, dass Anträge auf Beihilfefähigkeit einer psychotherapeutischen Behandlung dort formlos zu stellen seien, vom Dienstleister die rechtlichen Voraussetzungen geprüft würden und anschließend von der Beihilfefestsetzungsstelle entschieden würden, wobei der Entscheidung ein Magistratsbeschluss vorausgehe.

Ein solches Verfahren ist grundlegend unzulässig und lässt datenschutzrechtliche Maßstäbe vollkommen außer Acht.

Rechtliche Bewertung

Für den Antrag auf Anerkennung der Beihilfefähigkeit einer Psychotherapie ist nach den Verwaltungsvorschriften Nr. 5 zu § 6 Abs. 1 Nr. 1 Hessische Beihilfenverordnung (HBeihVO) ein förmliches Voranerkennungsverfahren vorgeschrieben, das auch ein Gutachterverfahren einschließt.

Demnach sind Aufwendungen für eine psychotherapeutische Behandlung dann beihilfefähig, wenn die **Festsetzungsstelle** vor Beginn der Behandlung die Beihilfefähigkeit der Aufwendungen aufgrund einer vertrauensärztlichen Stellungnahme zur Notwendigkeit und zu Art und Umfang der Behandlung anerkannt hat.

Festsetzungsstelle ist das Personalamt, das häufig im Hauptamt einer Gemeinde/Stadt integriert ist. Die Entscheidung über die Beihilfefähigkeit der Maßnahme ist von dem Sachbearbeiter/der Sachbearbeiterin, dem/der diese Aufgabe übertragen wurde (nicht dem Personalsachbearbeiter), auf Grundlage des einzuholenden Gutachtens zu treffen. Der als nicht ausreichend empfundene Datenschutz im Gutachterverfahren hat in der Vergangenheit immer wieder Anlass zu Beschwerden gegeben. Daher hat das Hessische Ministerium des Innern und für Sport auf die Anregungen meiner Behörde reagiert, 2013 das hierfür zu praktizierende Verfahren hessenweit geändert und an datenschutzorientierte Maßstäbe angepasst. Wie der hier vorgestellte Fall zeigt, werden die datenschutzgerechten neuen Antragsformulare noch nicht überall eingesetzt. Die „neuen“ Anträge sind z. B. auf der Webseite des Regierungspräsidiums Kassel www.rp-kassel.de Navigation Beihilfen abrufbar.

Folgendes Verfahren ist anzuwenden:
Bei der Beihilfefestsetzungsstelle ist der „neue“ Antragsbogen (Anlage 1) einzureichen. Die Seiten 1 und 2 mit den persönlichen Daten der/des Beihilfeberechtigten verbleiben ausschließlich bei der Beihilfestelle. Seite 2 ist immer eine Leerseite, die technisch sicherstellt, dass auch bei doppelseitigem Kopieren oder Scannen keine personenbezogenen Daten weitergegeben werden. An die Gutachterin/den Gutachter werden nur die übrigen Seiten (3 bis 5) in anonymisierter Form weitergeleitet.

Der Bericht der behandelnden Therapeutin/des Therapeuten in einem verschlossenen Umschlag und ein eventuell beigezogener Konsiliarbericht (Anl. 2 und 3) werden ebenso anonymisiert wie der Vordruck für die gutachterliche Stellungnahme (Anl. 4) und der dazugehörige, an die Festsetzungsstelle voradressierte Rückumschlag. Die Beihilfefestsetzungsstelle erlangt keine Kenntnis über den Inhalt einer Diagnose oder eventueller Therapievorschläge, sondern ausschließlich über die Tatsache, dass ein Antrag gestellt worden ist, über den sie zu entscheiden hat, und dass die hierzu eingereichten Belege vollständig sind. Die von der Gutachterin bzw. dem Gutachter verfasste Stellungnahme enthält keine inhaltliche Beschreibung des Behandlungsfalles. Sie enthält ausschließlich eine Empfehlung der zu genehmigenden Anzahl der Sitzungen, im anderen Fall die Empfehlung einer Ablehnung der Beihilfefähigkeit. Dieses Gutachten ist Grundlage für die Entscheidung der Festsetzungsstelle. Eine Kopie des Gutachtens geht der Therapeutin oder dem Therapeuten direkt über die Gutachterin bzw. den Gutachter zu. Der Genehmigungs- oder Ablehnungsbescheid wird von der Beihilfefestsetzungsstelle somit alleine aufgrund der medizinischen Empfehlung der Gutachterin bzw. des Gutachters verfasst, einen Ermessensspielraum gibt es nicht.

Der Genehmigungs- oder Ablehnungsbescheid wird an die Privatanschrift der/des Betroffenen übersandt. Eine Versendung über die Dienststelle per Dienstpost findet keinesfalls statt. Hierdurch wird sichergestellt, dass eine Kenntniserlangung von Vorgesetzten aufgrund der Nutzung des internen Postwegs ausgeschlossen ist. In diesem Zusammenhang weise ich darauf hin, dass Beihilfeakten stets als Teilakten zu führen sind und von den Personalakten getrennt aufzubewahren sind (§ 87 Abs. 1 HBG). Eine Übermittlung von Beihilfedaten an die Personalabteilung des Dienstherrn durch die Beihilfestelle ist nicht zulässig.

Datenschutzrechtlich unzulässig war vor allem die Übermittlung besonderer personenbezogener Daten, nämlich der Gesundheitsdaten des Betroffenen, an die Magistratsmitglieder der Stadt und an weitere Personen, deren Kenntniserlangung jeweils nicht erforderlich war.

Das in der Stadt praktizierte Verfahren, die Entscheidung über die Beihilfefähigkeit einer Maßnahme von einem Magistratsbeschluss abhängig zu machen, stellt einen groben Verstoß gegen datenschutzrechtliche Bestimmungen dar, hier des § 34 Abs. 1 HDSG. Diesen Verstoß habe ich ausdrücklich beanstandet und die Stadt aufgefordert, umgehend das oben beschriebene zulässige Verfahren anzuwenden.

Die für die Stadt zuständige Kommunalaufsichtsbehörde wurde verständigt.

Aufgrund meiner Hinweise wird die Stadt künftig die Verfahrensabläufe im Beihilfeverfahren ändern. Der Magistrat wird nicht mehr bei Entscheidungen über die Beihilfefähigkeit geplanter Maßnahmen beteiligt werden. Bei psychotherapeutischen Behandlungen wird künftig das Voranerkennungsverfahren nach dem Muster des Regierungspräsidiums Kassel beachtet werden.

Durch die vorgesehenen Änderungen gehe ich davon aus, dass die betroffene Stadt die datenschutzrechtlichen Bestimmungen, die für die Anerkennung der Beihilfefähigkeit von psychotherapeutischen Maßnahmen gelten, künftig einhalten wird.

7. Bilanz

7.1
Änderung des Hochschulgesetzes: Verordnung des HMWK zur Datenverarbeitung bei Forschungsinformationssystemen
(44. Tätigkeitsbericht, Ziff. 3.1.2)

Im 44. Tätigkeitsbericht hatte ich über meine Stellungnahme zur Novellierung des Hessischen Hochschulgesetzes (HHG) berichtet. Dabei ging es u. a. um die Schaffung einer gesetzlichen Regelung zur Einführung von Forschungsinformationssystemen an den hessischen Universitäten und Hochschulen. Meinen Vorschlag hatte das Ministerium aufgegriffen und eine Regelung in das Hessische Hochschulgesetz aufgenommen.

In der Folge war nun eine Konkretisierung der Verarbeitung personenbezogener Daten von Angehörigen der Hochschulen im Zusammenhang mit der Einrichtung und dem Betrieb von Forschungsinformationssystemen geboten. Hierzu hat mir das Ministerium den „Entwurf einer Verordnung über den Betrieb von Forschungsinformationssystemen“ zur Kenntnis gegeben und mich um eine datenschutzrechtliche Bewertung gebeten.

Die Verordnung regelt den Umfang der Verarbeitung personenbezogener Daten beim Betrieb von Forschungsinformationssystemen. In § 2 der Verordnung sind die einzelnen Merkmale genannt, die auch ohne Einwilligung der Betroffenen verarbeitet werden dürfen. Dabei handelt es sich u. a. um Personalstammdaten, forschungsbezogene Daten, insbesondere zu Projekten und Projektanträgen, Publikationen sowie Rahmendaten zu Drittmittelforschung usw.

Die Daten können nach § 3 der Verordnung von den Hochschulen auch unmittelbar aus den Personal-, Finanz- und Studierendendatensystemen übernommen werden.

In der Begründung zur Verordnung wird darauf verwiesen, dass Forschungsinformationssysteme insbesondere für die Erfüllung von Berichtspflichten für die Forschungsevaluation sowie für die interne forschungsadministrative Prozessabwicklung innerhalb von Hochschulen notwendig sind. Rechtlich abgedeckt wird dies durch die Regelungen in den §§ 12 Abs. 4 und 61 Abs. 3 HHG (Berichtswesen) und § 12 Abs. 1 HHG (Forschungsevaluation).

Damit ist den datenschutzrechtlichen Anforderungen hinsichtlich einer tragfähigen, bereichsspezifischen Rechtsgrundlage entsprochen.

7.2
Bereitstellung von Daten aus der Lehrer- und Schülerdatenbank für die Kirchen in Hessen
(43. Tätigkeitsbericht, Ziff. 4.1.8.1)

Die Bereitstellung zusätzlicher, personenbezogener Daten von Lehrkräften aus der LUSD an die Kirchen ist datenschutzrechtlich im Wesentlichen zulässig. Allerdings kann das Geburtsdatum nicht in Gänze den Kirchen zur Verfügung gestellt werden.

In meinem 43. Tätigkeitsbericht hatte ich über die Bereitstellung von personenbezogenen Daten aus der Lehrer- und Schülerdatenbank (LUSD) an die Kirchen berichtet. Das Verfahren soll als Abrufverfahren mit Online-Zugriff konzipiert werden. Vom HKM wird aus der LUSD auf Grundlage des Erlasses vom 19.12.2008 (ABl. 1/09) ein Datensatz generiert, welcher in einem gesonderten Verzeichnis auf einem Server der Hessischen Zentrale für Datenverarbeitung (HZD) liegt. Ein wie auch immer gearteter unmittelbarer Zugriff auf die Daten der LUSD ist ausgeschlossen.

Rechtsgrundlage hierfür ist einerseits § 83 Abs. 1 HSchG, wonach eine Übermittlung personenbezogener Daten an andere öffentliche Stellen zulässig ist, soweit die Kenntnis der Daten zur Erfüllung der dem Empfänger durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist. Zum anderen sind im Erlass vom 19.12.2008 die Merkmale, welche den Kirchen zur Verfügung gestellt werden, konkretisiert. Dabei stellte ich fest, dass der Umfang der Datenlieferung umfangreicher war, als es der Erlass vorsah. Insbesondere handelte es sich um die Merkmale Geburtsdatum sowie private Anschrift der betroffenen Lehrkräfte. Ich musste seinerzeit darauf bestehen, dass diese Merkmale nicht weiter übermittelt werden. Außerdem wies ich darauf hin, dass, soweit es nachweislich ein Erfordernis für die Nutzung gäbe, der Erlass um weitere Merkmale angereichert werden könne.

In einem weiteren Gespräch meines Mitarbeiters mit den Vertretern der Kirchen in Hessen sowie dem HKM wurde diese Position nochmals ausdrücklich betont. Daraufhin erstellten die Kirchenvertreter eine ausführliche Stellungnahme hinsichtlich der Notwendigkeit zur Lieferung dieser beiden zusätzlichen Merkmale.

Hinsichtlich des Geburtsdatums der Betroffenen konnte mich der Schriftsatz der Kirchen nur teilweise überzeugen. Für Zwecke der Personalplanung und des Personaleinsatzes für den Religionsunterricht ist das Geburtsjahr in der Tat wesentlich. Tages- bzw. monatsscharf dieses Datum erhalten zu müssen, erscheint mir jedoch nicht schlüssig, zumal die Kirchen selbst in ihrem Schriftsatz die Erforderlichkeit des kompletten Geburtsdatums in Frage stellten.

Bei der privaten Anschrift geht es um die direkte Kommunikation mit den Lehrkräften, um Einladungen auf der Ebene der Pfarrverbünde und Dekanate versenden und Informationen weiterleiten zu können. Außerdem könnten Unterstützungsangebote zur Aktualisierung der fachlichen Kompetenzen und zur Unterstützung der Lehrkräfte bei spezifischen unterrichtlichen Belastungssituationen kommuniziert werden. Da es bislang bei der über die jeweilige Schule vorgenommenen Kontaktaufnahme immer wieder zu Rückläufern oder einer verzögerten Zustellung an die Betroffenen kam, versprechen sich die Kirchen von einer unmittelbaren Ansprache eine schnellere Resonanz. Dieser Argumentation konnte ich mich nicht verschließen und habe deshalb einer Bereitstellung dieses Datums zugestimmt. Erforderlich ist aber die Ergänzung des Erlasses.

Das HKM muss diesen Erlass auf den Weg bringen, in dem die Modalitäten für das Online-Verfahren geregelt und die zusätzlichen, personenbezogenen Merkmale aufgenommen sind.

7.3

Sicherung von Patientenakten nach Schließung von Krankenhäusern (43. Tätigkeitsbericht, Ziff. 3.1.1; 44. Tätigkeitsbericht, Ziff. 6.2)

In den vergangenen beiden Tätigkeitsberichten habe ich wiederholt über die aktuellen Entwicklungen zum Thema Lagerung von Patienten- und Personalakten bei Schließung einer Gesundheitseinrichtung berichtet. Auch in diesem Jahr möchte ich wieder über aktuelle Sachverhalte und Entwicklungen berichten.

7.3.1

Aktueller Sachstand

Die Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden (AOLG) hat sich in ihrer 36. Sitzung zu dem Thema „Gesetzliche Regelung zur Aufbewahrung von Patientenakten“ dazu entschlossen, bei der im Jahr 2016 stattfindenden Gesundheitsministerkonferenz (GMK) einen Beschlussvorschlag zu diesem Thema einzureichen. Bei der 89. Gesundheitsministerkonferenz am 29./30.06.2016 wurde nunmehr unter TOP 11.2 „Gesetzliche Regelung zur Aufbewahrung von Patientenakten“ beschlossen:

„Die GMK sieht aktuellen Handlungsbedarf bei dem Umgang mit Patientenakten geschlossener, insbesondere insolventer Einrichtungen, wie z. B. Krankenhäuser und Reha-Einrichtungen, die Patientenakten verwalten, und bittet die Bundesregierung, umgehend eine Gesetzesinitiative, z. B. zum Bürgerlichen Gesetzbuch (BGB), in die Wege zu leiten, damit das Recht der Patientinnen und Patienten auf Akteneinsichtnahme gemäß § 630g BGB gesichert ist.“

Aktuell ist hier nicht bekannt, in welcher Form dieser Beschluss bereits aufgegriffen wurde. Erfreulich ist jedoch, dass hier offenbar einstimmig ein Handlungsbedarf festgestellt wurde.

7.3.2

Entwicklungen auf Landesebene

Zwischenzeitlich sind unterdessen auch weiterhin Meldungen aus anderen Bundesländern eingegangen, wonach dort die Patientenakten in mittlerweile geschlossenen Kliniken nicht hinreichend gesichert waren. Ein bekanntes Beispiel ist hier zum Beispiel die frühere Wiedemann-Klinik in Ambach. Den Pressemeldungen zufolge lagen offenbar jahrelang in den maroden Gebäuden Akten und Röntgenbilder frei herum. Besondere Brisanz erhielt dieser Fall dadurch, dass auch viele Prominente Patienten dieser Klinik waren, so unter anderem Klausjürgen Wussow, Inge Meysel, Heinz Rühmann und Harald Juhnke.

7.3.3

Ausblick

Gemäß meiner Rücksprache mit dem Hessischen Ministerium für Soziales und Integration ist es geplant, in die Novellierung des Hessischen Krankenhausgesetzes im Frühjahr 2017 eine Regelung aufzunehmen, wonach Krankenhäuser in Hessen für eine entsprechende Konstellation (Schließung, Insolvenz) bereits im Vorfeld Vorkehrungen dafür zu treffen haben, dass die weitere Aufbewahrung und Sicherung der Patientenakten sichergestellt ist. Zudem teilte mir das Hessische Ministerium für Soziales und Integration mit, dass man noch einmal alle Krankenhäuser, in denen Abteilungen geschlossen wurden, anschreiben möchte, um abzuklären, in welcher Weise die sichere Aufbewahrung der Daten und ihre Verfügbarkeit für die Patienten sichergestellt ist.

7.4

Kopiergeräte am Ende des Mietvertrages: Was geschieht mit den Daten? (36. Tätigkeitsbericht, Ziff. 6.1.2.2 und Ziff. 8.2.4)

Beim Einsatz digitaler Kopierer ergeben sich für die Betreiber und Leasinggeber dieser Geräte Verpflichtungen, die gespeicherten Daten sorgsam gegen unbefugte Zugriffe Dritter zu schützen bzw. am Vertragsende fachgerecht zu löschen.

Bis zur Entwicklung digitaler Kopiergeräte wurden mit den verwendeten Geräten keine Zwischenspeicherungen der Vorlagen erzeugt. Für eine zweite Kopie musste das Original erneut belichtet werden. Mit der digitalen Technik wird demgegenüber zunächst ein Scan vom Original erzeugt, der als Bilddatei auf einem Speichermedium zumeist einer Festplatte abgelegt wird. Da moderne digitale Kopiergeräte in aller Regel als Multifunktionsgeräte eingesetzt werden, wird die Speicherkomponente aber auch in allen anderen Zusammenhängen für weitere Zugriffe auf gescannte Vorlagen sowie gedruckte Bilder und Dokumente genutzt.

Um während des Nutzungszeitraums Zugriffe auf die gespeicherten Daten auf einen Kreis sachlich zuständiger Personen zu beschränken, haben die Hersteller verschiedene Softwareergänzungen in ihre Angebote aufgenommen, die der jeweiligen Betriebssituation gerecht werden sollen.

Auch für den Zeitpunkt am Ende des Vertrages bieten die Lieferanten einige Optionen. Ein Standard ist die Variante, bei der dem Kunden ein fachgerechtes Löschen der Festplatte – nach einem anerkannten Stand der Technik – zugesichert wird; ggf. wird auch die Vernichtung des Speichermediums durch ein zertifiziertes Unternehmen angeboten.

Der Südwestrundfunk (SWR) hat in einem Beitrag die Probe aufs Exempel gemacht und sich mehrere Geräte auf dem Gebrauchtgerätemarkt im Internet besorgt. Bei drei Geräten waren die Daten aus den vorherigen Nutzungen tatsächlich noch vorhanden und konnten mit einer frei verfügbaren Software an einem Standard-PC ausgelesen werden. Einer dieser Kopierer erwies sich als besonders heikler Fall. Die Kopien und Scanvorgänge enthielten die Daten aus Strafbefehlen, Mahnverfahren, polizeilichen Vernehmungsprotokollen sowie Gehalts-, Steuer- und Kontodaten und führten nach Recherchen der SWR-Redaktion zu einer Rechtsanwaltskanzlei, bei der das Kopiergerät zuletzt im Einsatz war. Der Anwalt bezog sich auf Nachfrage der Redaktion darauf, dass er die fachgerechte Löschung der Daten zum Vertragsbestandteil gemacht habe und der Auftragnehmer habe vertragswidrig diese Maßnahme nicht umgesetzt. Ein fachgerechtes Löschen erfordert aber auch eine Dokumentation des Vorganges, aus der hervorgeht, welcher Datenträger durch wen, wann und mit welcher Methode gelöscht oder vernichtet wurde. Gerade Berufsgeheimnisträger wie Anwälte, Ärzte oder andere in § 203 StGB genannte Personen sollten dem höheren Schutzbedarf der ihnen anvertrauten Geheimnisse in besondere Weise Rechnung tragen und sich zur Wahrung ihrer Sorgfaltspflicht eine Ausfertigung dieser Dokumentation aushändigen lassen.
Das Löschen der Daten wäre in den vom SWR aufgezeigten Fällen unter diesen Umständen sicherlich auch nicht unterblieben.

Wer ganz sicher gehen will, wählt eine Vertragsoption, bei der das Speichermedium zum Vertragsende vor der Abholung der Geräte in den Besitz des Auftraggebers übergeht, um die darauf folgende Löschung oder Vernichtung persönlich oder durch eine beauftragte Person zu begleiten. Hier bleibt die Kontrolle über die Daten bis zu deren Löschung vollständig in der Verantwortung der datenverarbeitenden Stelle.

8. Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

8.1

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 06./07.04.2016

Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell *), dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

*)
- Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster
- Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg
- Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München
- Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

8.2

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 06./07.04.2016

Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So sind dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt dies insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.
- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.
- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogene Daten als auch das Konto selbst löschen zu lassen.
- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default" eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die länderübergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

8.3
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 06./07.04.2016

Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.
- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

8.4

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 06./07.04.2016

Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i. V. m. Erwägungsgrund [EG] 155),
- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i. V. m. EG 53, letzte beiden Sätze),
- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i. V. m. EG 150, vorletzter Satz),
- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4f Abs.1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

8.5

Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20.04.2016

Klagerecht für Datenschutzbehörden – EU-Kommissionsentscheidungen müssen gerichtlich prüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den "EU-US Privacy Shield" bestehen jedoch nach Auffassung der Artikel 29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel 29-Datenschutzgruppe hat zum "EU-US Privacy Shield" zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der "EU-US Privacy Shield" in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner oben genannten Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BRDrucks. 171/16), in der nochmals deutlich gemacht wird, "dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6.10.2015; Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist."

8.6

Umlaufentschließung[1)] der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25.05.2016

EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),
- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),
- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,
- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,
- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),
- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,
- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,
- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

---

1) bei Enthaltung Bayerns (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht)

8.7

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 10.11.2016

Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf; Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[1] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift" (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:
- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Abs. 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:
1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.
2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.
3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

---

[1] bei Enthaltung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit

8.8

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 10.11.2016

"Videoüberwachungsverbesserungsgesetz" zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein "Videoüberwachungsverbesserungsgesetz" Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur

Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[1] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

[1] bei Enthaltung der Bundesbeauftragten für Datenschutz und Informationsfreiheit

9. Beschluss des Düsseldorfer Kreises

9.1

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13./14.09.2016

Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit ("Kopplungsverbot", Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),

- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

10. Materialien

10.1

Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz

Stand: Januar 2016

Die Orientierungshilfe zeigt den datenschutzrechtlichen Rahmen und Regelungsmöglichkeiten der Nutzung des betrieblichen Internet- und E-Mail-Dienstes durch die Beschäftigten auf. Sie soll es den Arbeitgebern und den Beschäftigten erleichtern, eine klare Regelung im Unternehmen zu erreichen, soweit eine private Nutzung des Internets und/oder des E-Mail-Dienstes erlaubt sein soll. Zudem enthält diese Orientierungshilfe ein Muster für eine Betriebsvereinbarung/Richtlinie/Anweisung für die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfachs.

Inhaltsverzeichnis

Muster einer Betriebsvereinbarung für die private Nutzung des Internets und des betrieblichen E-Mail-Postfachs

A. Allgemeines

I. Überblick

„Darf ich am Arbeitsplatz privat das Internet nutzen? Darf ich am Arbeitsplatz private E-Mails versenden?“ – diese Fragen haben viele Beschäftigte, die Zugang zum Internet haben.

Für den Arbeitgeber stellen sich ähnliche Fragen: *„Darf ich auf das E-Mail-Postfach der Beschäftigten zugreifen, wenn sie ungeplant abwesend sind? Darf ich die Internetnutzung kontrollieren? Welche Gestaltungsmöglichkeiten habe ich im Voraus?“*

Datenschutzrechtlich bedeutsam sind in diesem Zusammenhang die anfallenden personenbezogenen Daten, und zwar sowohl der Beschäftigten als auch ihrer Kommunikationspartner und anderer Betroffener (z. B. Dritter, deren Namen in einer E-Mail genannt wird).

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit der E-Mail- und Internetnutzung am Arbeitsplatz ist es sehr relevant, ob den Beschäftigten auch die private Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs am Arbeitsplatz gestattet worden ist.

Diese Orientierungshilfe stellt einige der hierbei zu beachtenden datenschutzrechtlichen Anforderungen dar und zeigt Regelungsmöglichkeiten auf. Sie richtet sich an die Wirtschaft und kann in der Regel entsprechend für den öffentlichen Dienst angewendet werden. Landesspezifische Vorschriften sind zu beachten.

Im Anhang befindet sich das Muster einer Betriebsvereinbarung und ergänzender Einwilligung, mit der die private Internet- und E-Mail-Nutzung geregelt werden kann. Das Muster kann auch als Beispiel genommen werden, um diese Punkte in eine Anweisung/Richtlinie oder in den einzelnen Arbeitsvertrag aufzunehmen.[1] Dies bietet sich insbesondere dann an, wenn es im Unternehmen keinen Betriebsrat gibt. Das Muster ist an die konkreten Gegebenheiten im jeweiligen Unternehmen anzupassen; zudem sind jeweils arbeitsrechtliche Fragestellungen zu beachten, die dieses Papier nicht erschöpfend berücksichtigen kann.

II. Rechtlicher Rahmen

1. Grundsatz

Soweit der Arbeitgeber Hardware bzw. Software zur Verfügung stellt, dürfen die betrieblichen Internet- und E-Mail-Dienste grundsätzlich nur für die betriebliche Tätigkeit genutzt werden. Eine private Nutzung von Internet und/oder betrieblichem E-Mail-Postfach ist daher nicht erlaubt, es sei denn, der Arbeitgeber hat eine Privatnutzung ausdrücklich z. B. im Arbeitsvertrag oder in einer Betriebsvereinbarung geregelt oder, was überwiegend als möglich angesehen wird, in Kenntnis und Duldung der privaten Nutzung über einen längeren Zeitraum (sog. „betriebliche Übung“) konkludent genehmigt.

Dem Arbeitgeber steht es frei, ob er eine Privatnutzung des Internets und/oder des betrieblichen E-Mail-Accounts erlaubt.

2. Gesetzlicher Rahmen

a) BDSG und Arbeitsrecht

Soweit die Nutzung des Internets und/oder des betrieblichen E-Mail-Postfachs ausschließlich zu betrieblichen Zwecken erlaubt ist, richtet sich die Erhebung, Verarbeitung und Nutzung von anfallenden personenbezogenen Daten nach dem Bundesdatenschutzgesetz (BDSG).
Da sich das öffentlich-rechtliche Datenschutzrecht gemäß BDSG, welches Gegenstand dieser Orientierungshilfe ist, und das zivilrechtliche Arbeitsrecht „überlappen“, sind parallel arbeitsrechtliche Fragestellungen zu berücksichtigen.

b) TKG und TMG

Wenn der Arbeitgeber den Beschäftigten auch die private Nutzung von Internet und/oder des betrieblichen E-Mail-Postfachs erlaubt, ist zusätzlich das Telekommunikationsgesetz (TKG) bzw. das Telemediengesetz (TMG) zu beachten. Nach Auffassung der Aufsichtsbehörden ist der Arbeitgeber in diesem Fall Telekommunikationsdienste- bzw. Telemediendienste-Anbieter. Dies hat die Konsequenz, dass er an das Fernmeldegeheimnis des § 88 Abs. 2 S. 1 TKG gebunden ist und gemäß § 11 Abs. 1 Nr. 1 TMG den Datenschutzvorschriften des TMG unterliegt. Zugleich bedeutet dies, dass sich der Arbeitgeber bei einer Verletzung des Fernmeldegeheimnisses gemäß § 206 Strafgesetzbuch (StGB) strafbar machen kann.

Zum rechtlichen Hintergrund: Das Fernmeldegeheimnis kann sich auch auf E-Mails erstrecken, die auf einem Server des jeweiligen Diensteanbieters zwischen- oder endgespeichert sind. Daher wird auch der „ruhende“ E-Mail-Verkehr erfasst, bei dem ein „dynamischer“ Telekommunikationsvorgang nicht (mehr) stattfindet (BVerfG, 16.6.2009, 2 BVR 902/06). Solange also E-Mails im Herrschaftsbereich des jeweiligen Diensteanbieters verbleiben, folgt die Schutzbedürftigkeit der Kommunikationspartner aus dieser Einschaltung eines Dritten.

Einige Gerichte vertreten demgegenüber die Auffassung, dass Arbeitgeber, die die private Nutzung des Internets und/oder eines betrieblichen E-Mail-Postfachs gestatten oder dulden, nicht als Diensteanbieter im Sinne des TKG bzw. TMG anzusehen sind und daher nicht dem Fernmeldegeheimnis unterliegen.[2]

Solange jedoch diese Frage nicht höchstrichterlich oder durch den Gesetzgeber eindeutig geklärt ist, sollten Arbeitgeber zur Vermeidung etwaiger Strafbarkeit davon ausgehen, Diensteanbieter zu sein. Hiervon geht auch die vorliegende Orientierungshilfe aus.

Auf die Verpflichtung des Arbeitgebers, die Beschäftigten über die Erstellung von Einzelverbindungsnachweisen und deren Kenntnisnahme gemäß § 99 Abs. 1 Satz 4 TKG zu informieren, wird hingewiesen.

B. Ausschließlich betriebliche Nutzung

I. Internet

1. Der Arbeitgeber hat grundsätzlich das Recht, anhand von Protokolldaten stichprobenartig[3] zu prüfen, ob das Surfen der Beschäftigten betrieblicher Natur ist. Dazu ist es in einem ersten Schritt zulässig und ausreichend, wenn sie für diesen Zweck zunächst nur eine Auswertung des Surfverhaltens ohne Personenbezug vornehmen, d. h. insbesondere auch ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung der einzelnen Beschäftigten. Grundsätzlich ist datenschutzfreundlichen Maßnahmen – z. B. Nutzung von black- und/oder whitelists – der Vorzug zu geben. Für die Erstellung solcher black- bzw. whitelists können hinsichtlich der Internetnutzung wirksam anonymisierte Protokolldaten herangezogen werden. Eine personenbezogene Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten unter den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG bei konkretem Missbrauchsverdacht im verhältnismäßigen Rahmen zulässig. Danach können zur Aufdeckung von Straftaten personenbezogene Daten der Beschäftigten erhoben, verarbeitet oder genutzt werden, wenn folgende Voraussetzungen vorliegen: Es müssen zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Betroffenen im Beschäftigungsverhältnis eine Straftat begangen haben. Zudem muss die Maßnahme zur Aufdeckung erforderlich sein. Letztlich darf nicht das schutzwürdige Interesse der Betroffenen überwiegen; insbesondere dürfen Art und Ausmaß nicht unverhältnismäßig sein.

2. Soweit im Zusammenhang mit der Nutzung des Internets personenbezogene Daten anfallen, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebs der Verfahren gespeichert werden, dürfen diese Daten auch nur zu diesen Zwecken genutzt werden (§ 31 BDSG). Eine Nutzung dieser Daten zur Verhaltens- und Leistungskontrolle der Beschäftigten ist nicht erlaubt.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ein- und ausgehende betriebliche E-Mails der Beschäftigten darf der Arbeitgeber zur Kenntnis nehmen. Beispielsweise kann er verfügen, dass die Beschäftigten ihm jede für den Geschäftsgang relevante oder fest definierte ein- oder ausgehende E-Mail einzeln zur Kenntnis zuleiten. Eine durch den Arbeitgeber eingerichtete automatisierte Weiterleitung aller ein- und ausgehenden E-Mails an einzelne Vorgesetzte ist, sofern arbeitsrechtlich nicht statthaft, auch datenschutzrechtlich mangels Erforderlichkeit unzulässig (Verbot der permanenten Kontrolle).

2. Für den Fall der Abwesenheit kann eine Weiterleitung der E-Mail in Betracht kommen. Allerdings sollte im Hinblick auf die schutzwürdigen Belange der Beschäftigten die Verwendung eines Abwesenheitsassistenten vorgezogen werden. Aufgrund der schutzwürdigen Belange der Beschäftigten stellt dieses Vorgehen das mildeste Mittel dar. Nur wenn eine Abwesenheitsmitteilung nicht ausreicht, kann eine Weiterleitung in Betracht gezogen werden.

Auf bereits empfangene bzw. versandte betriebliche E-Mails darf der Arbeitgeber nur zugreifen, wenn dies für betriebliche Zwecke erforderlich ist.

3. E-Mails dürfen von dem Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter erkannt wurde. Etwas anderes kann im Falle erforderlicher Maßnahmen der Missbrauchskontrolle gelten.

4. a) Zur Missbrauchskontrolle gelten die Ausführungen zu B I 1 entsprechend.
b) Zur Regelung des § 31 BDSG (besondere Zweckbindung erhobener Daten) gelten die Ausführungen zu B I 2 entsprechend.

C. Private Nutzung

I. Internet

1. Ist die private Nutzung des Internets erlaubt (oder gilt sie als erlaubt, s. o. 4), wird der Arbeitgeber hinsichtlich der privaten Nutzung zum Diensteanbieter im Sinne des TKG und unterliegt den Datenschutzbestimmungen des TMG. Er ist daher grundsätzlich zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen (Protokolldaten), ist dem Arbeitgeber nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Dies betrifft insbesondere die Daten, aus denen sich ergibt, welche Internetseiten welche Beschäftigten wann aufgerufen haben. Ausnahmen gelten allerdings gemäß §§ 88 Abs. 3, 91 ff. TKG (z. B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d. h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis einer Privatnutzung an Bedingungen knüpfen: Es bieten sich insbesondere Regelungen zum zeitlichen Umfang der Privatnutzung an. Auch konkrete Verhaltensregeln sollten vor Beginn der privaten Nutzung getroffen werden. Der Arbeitgeber braucht in diesem Zusammenhang eine Einwilligung der Beschäftigten, die sich darauf bezieht, dass diese mit Zugriffen des Arbeitgebers (wie unter 1. beschrieben) einverstanden sind. Die Einwilligung erstreckt sich also auf Art und Umfang von Zugriffen und Kontrollen. Diese Kontrollen umfassen die Einhaltung der Nutzungsregelungen (zeitlicher Umfang bzw. Inhalt der Nutzung).

3. Zur Einwilligung: Auf der „ersten Stufe“ sollte eine Betriebsvereinbarung abgeschlossen werden. In dieser sollte der Gegenstand der späteren, individuellen Einwilligungen umrissen werden. Sodann sind auf dieser Grundlage die individuellen Einwilligungen der einzelnen Beschäftigten einzuholen.

Die Einwilligung sollte gesondert erklärt werden. Den Beschäftigten ist vor der Einwilligung Gelegenheit zu geben, die Betriebsvereinbarung zur Kenntnis zu nehmen.

4. Zum weiteren Inhalt einer Betriebsvereinbarung: Es ist zu empfehlen, sämtliche Fragen zur Privatnutzung in der Betriebsvereinbarung zu regeln. In der Betriebsvereinbarung sollten daher die Nutzungsregelungen (zeitlicher Umfang, Verhaltensregeln) und die Zugriffsmöglichkeiten (Einwilligung, insbesondere zu Art und Umfang von Kontrollen) eindeutig festgehalten sein.

5. Auf der Grundlage der Einwilligung darf eine Protokollierung der Internetnutzung sowie eine Auswertung der Protokolldaten entsprechend B.I. stattfinden. Eine personenbezogene Auswertung von Protokolldaten darf jedoch nur bei einem konkreten Verdacht erfolgen. In Betracht kommt insbesondere der Verdacht eines Verstoßes gegen in der Betriebsvereinbarung festgeschriebene Verhaltensvorschriften bzw. den festgelegten Umfang der erlaubten Privatnutzung. Eine personenbezogene Kontrolle ist nur zulässig, wenn sie verhältnismäßig ist.

6. Beschäftigte, die diese Bedingungen nicht akzeptieren wollen, können ihre Einwilligung ohne jeden arbeitsrechtlichen Nachteil verweigern. Eine Privatnutzung ist dann nicht erlaubt. Da für diese Beschäftigten im Ergebnis nur die betriebliche Nutzung erlaubt ist, gelten für sie die Ausführungen unter B.I.

II. Nutzung des betrieblichen E-Mail-Accounts

1. Ist die private E-Mail-Nutzung erlaubt (oder gilt sie als erlaubt, s. o. 5), ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet.

Der Schutz des Fernmeldegeheimnisses gilt, solange der Übermittlungsvorgang andauert und die E-Mail noch nicht in den ausschließlichen Herrschaftsbereich des Empfängers gelangt ist. Dies ist beispielsweise der Fall, wenn sie sich noch in einem E-Mail-Postfach auf dem Server im Zugriffsbereich des Arbeitgebers befindet. Der Abschluss des Übermittlungsvorgangs hängt von den technischen

Gegebenheiten, insbesondere dem verwendeten Übertragungsprotokoll, ab. Solange Nachrichten – wie bei Verwendung des „IMAP-Protokolls“ – auf einem zentralen E-Mail-Server des Arbeitgebers oder eines Providers verbleiben und bei jedem Zugriff durch die Beschäftigten erneut heruntergeladen werden, ist der Übermittlungsvorgang nicht beendet. Dies hat zur Folge, dass der Arbeitgeber grundsätzlich ohne Einwilligung der jeweiligen Beschäftigten nicht auf deren betriebliches E-Mail-Postfach zugreifen darf.

Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten erlaubt. Allerdings gelten gemäß §§ 88 Abs. 3, 91 ff. TKG die dort geregelten Ausnahmen (z. B. erforderliche Maßnahmen zum Schutz der technischen Systeme, d. h. zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen).

2. Der Arbeitgeber kann die Erlaubnis zur privaten Nutzung des betrieblichen E-Mail-Postfachs an Bedingungen knüpfen: In Betracht kommen Nutzungsregelungen (insbesondere zum zeitlichen Umfang; ggf. auch Verhaltensregeln) und Zugriffsmöglichkeiten des Arbeitgebers. Hierfür ist wiederum eine Einwilligung der Beschäftigten einzuholen. Wie schon bei der privaten Internetnutzung geht es hierbei zum einen um die Möglichkeit von Kontrollen (bezogen auf die o.g. Nutzungsregelungen). Die Einwilligung sollte sich daher auf Art und Umfang solcher etwaiger Kontrollen beziehen.

Im Gegensatz zur privaten Internetnutzung steht jedoch bzgl. des privaten Mailverkehrs eine andere Zugriffsmöglichkeit im Vordergrund: Im gemeinsamen betrieblichen Interesse sollte eindeutig im Vorfeld festgelegt werden, ob bzw. wie der Arbeitgeber auf die betrieblichen Mails im gemischt-privat-betrieblichen Postfach zugreifen kann.

Die Ausführungen unter C. I. 26 gelten hierfür entsprechend.

3. Der Arbeitgeber sollte also klare Vorgaben machen, welche Einstellungen die Beschäftigten vorzunehmen haben, wenn sie – geplant oder nicht geplant – abwesend sind (z. B. Abwesenheitsnotiz).

4. Wurden diese Einstellungen nicht vorgenommen (etwa weil es bei einer ungeplanten Abwesenheit nicht möglich war oder weil es vergessen wurde), darf ein Zugriff auf das betriebliche E-Mail-Postfach der betroffenen Beschäftigten, soweit dies für betriebliche Zwecke erforderlich ist, nur mit deren vorab eingeholter Einwilligung erfolgen.

5. Ein Zugriff auf bereits vor der Abwesenheit der jeweiligen Beschäftigten eingegangenen E-Mails ist ebenfalls nur zulässig, soweit dieser für betriebliche Zwecke erforderlich ist und vorab Einwilligungen der Beschäftigten eingeholt wurden.

6. Haben Beschäftigte im Zusammenhang mit der betrieblichen E-Mail-Nutzung in die Regelungen zur privaten Mailnutzung eingewilligt, sind sie darauf hinzuweisen, dass im Zusammenhang mit einer Archivierung (z. B. gemäß § 257 HGB, § 147 AO) auch eine Archivierung ihrer privaten E-Mails erfolgen kann. Den Beschäftigten sollte jedoch Gelegenheit gegeben werden, private Mails zu löschen oder an ihren privaten Account weiterzuleiten.

D. Regelungen für Geheimnisträger

„Geheimnisträger" in diesem Sinne sind Beschäftigte, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden (Betriebsrat, Jugend- und Ausbildungsvertretung, betrieblicher Datenschutzbeauftragter, Betriebsarzt, Gleichstellungsbeauftragte u. a.) und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen.

I. Internet

Grundsätzlich besteht keine Kontrollbefugnis des Arbeitgebers bzgl. der Internetnutzung der o. g. „Geheimnisträger“, z. B. der Betriebsräte.

II. Nutzung des betrieblichen E-Mail-Accounts

Bei den „Geheimnisträgern“ muss eine Kenntnisnahme des Arbeitgebers von den Verkehrs- und Inhaltsdaten ausgeschlossen werden. Es empfiehlt sich, für diese Stellen nicht personalisierte funktionsbezogene Postfächer (z. B. Betriebsrat@Unternehmen.de) einzurichten und diese von Kontrollen bzw. Auswertungen auszunehmen.

Neben den Belangen der „Geheimnisträger“ selbst sind in gleichem Maße die schutzwürdigen Belange der einzelnen Beschäftigten, die mit dem jeweiligen „Geheimnisträger“ kommunizieren, zu beachten. Auch insofern sind Vorkehrungen zu treffen. Es ist daher dafür zu sorgen, dass E-Mails der Beschäftigten von bzw. an den jeweiligen „Geheimnisträger“ (ggf. aufgrund einer einschlägigen Betreffzeile) von dem Arbeitgeber nicht zur Kenntnis genommen werden. Den Beschäftigten sollte daher empfohlen werden, derartige Kommunikation über andere Wege (z. B. private E-Mail-Adresse, schriftlich oder telefonisch) zu führen. So kann eine Kenntnisnahme der Verkehrs- und Inhaltsdaten durch den Arbeitgeber vollkommen ausgeschlossen werden.

E. Empfehlungen der Aufsichtsbehörden

1. Es wird empfohlen, über die betriebliche und/oder private Nutzung des Internets und des betrieblichen E-Mail-Accounts eine schriftliche Regelung zu treffen, in der die Fragen des Zugriffs, der Protokollierung, Auswertung und Durchführung von Kontrollen eindeutig festgelegt werden. Auf mögliche Überwachungsmaßnahmen und in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.

2. Sofern der Arbeitgeber seinen Beschäftigten die Möglichkeit zur Nutzung des betrieblichen E-Mail-Accounts für private E-Mail-Kommunikation ermöglichen möchte, sollte er bedenken, dass er dann an das Fernmeldegeheimnis gebunden ist. Dies führt in der Praxis regelmäßig zu erheblichen Konflikten, nämlich dann, wenn der Arbeitgeber für den Geschäftsablauf auf das betriebliche Postfach der Beschäftigten zugreifen möchte. Es wird daher empfohlen, dass der Arbeitgeber den Beschäftigten lediglich die private Nutzung des Internets anbietet, welche auch die Nutzung von Webmail-Diensten (wie z. B. web.de; gmx.de; yahoo.de etc.) umfasst. Anstatt der Nutzung der betrieblichen E-Mail-Accounts sollten die Beschäftigten dann auf die ausschließliche Nutzung privater Web-Mail-Accounts für private Nachrichten verwiesen werden. Das jeweilige betriebliche Postfach wird dann weiterhin ausschließlich betrieblich genutzt (vgl. B II).

3. Wenn der Arbeitgeber seinen Beschäftigten die private Nutzung des betrieblichen E-Mail-Accounts erlaubt hat (vgl. C II) und für den Geschäftsablauf auf das betriebliche Mailpostfach der einzelnen Beschäftigten zugreifen möchte, hat er Folgendes zu beachten: E-Mails mit erkennbar privatem Inhalt dürfen von dem Arbeitgeber nur in dem Umfang zur Kenntnis genommen werden, wie dies von der Einwilligung gedeckt und unerlässlich ist, um sie von den betrieblichen E-Mails zu trennen. Dasselbe gilt für solche E-Mails, die der Kommunikation der Beschäftigten mit „Geheimnisträgern“ (Betriebsrat, Jugend- und Ausbildungsvertretung, Schwerbehindertenvertretung, Gleichstellungsbeauftragte u. a.) dienen. Dies ist durch eine entsprechende Verfahrensgestaltung zu gewährleisten. Wenn sich im Rahmen der Sichtung aus dem Absender und/oder Betreff einer E-Mail Anhaltspunkte dafür ergeben, dass es sich um eine geschützte und dem Privatbereich zuzurechnende E-Mail handelt, ist der Vertreter der Arbeitgeber oder die von dem Arbeitgeber bestimmte Person nicht berechtigt, den Inhalt der E-Mail zur Kenntnis zu nehmen, zu verarbeiten oder zu nutzen.

4. Wenn Beschäftigte das Unternehmen verlassen, sollte darauf geachtet werden, dass die persönliche betriebliche E-Mail-Adresse schnellstmöglich deaktiviert wird.

5. Ergänzende Hinweise lassen sich den Orientierungshilfen „Protokollierung“ und „zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ entnehmen.

F. Spamfilter und Virenschutz

Aus Gründen der Datensicherheit dürfen Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie Inhalte aufweisen, die zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen können (Virenfilterung). Davon zu unterscheiden ist die Ausfilterung bzw. Veränderung von „Spam-Mails“. Beim Verfahren zur Behandlung von Spam-Mails ist § 303a StGB zu beachten.

1. Spamfilter

Über eine zentrale Spam-Filterung ist im Vorfeld zu unterrichten. Es gibt eine Vielzahl an Möglichkeiten zur Abwehr unerwünschter Nachrichten (Spam), die in verschiedensten Kombinationen und Ausprägungen eingesetzt werden können. Aus den in Betracht kommenden Varianten sollte die datenschutzfreundlichste gewählt werden. Zugleich sollte folgenden Grundsätzen Rechnung getragen werden:

- Filter, die Header oder Inhalt elektronischer Post automatisch auf unerwünschte Nachrichten (Spam) prüfen, sollten erst an einem Punkt eingesetzt werden, der außerhalb der Reichweite des Fernmeldegeheimnisses liegt.

- Die (zentrale) Markierung spamverdächtiger Nachrichten ist dabei der zentralen Löschung von E-Mails ohne Kenntnis des Empfängers vorzuziehen.
- Um Verletzungen von Vertraulichkeit und Integrität zu vermeiden, sollten die Empfänger der Nachrichten in größtmöglicher Autonomie selbst über den Umgang mit den an sie gerichteten E-Mails entscheiden können.

2. Virenschutz

Das Herausfiltern und Untersuchen von virenverseuchten E-Mails mit Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist hinsichtlich privater E-Mails nur in dem in § 100 TKG festgelegten Umfang gestattet.

Anhang 1:

Muster einer Betriebsvereinbarung für die private Nutzung des Internets

Hinweise:
- Entsprechend der Darstellung unter C.I. wird im folgenden Muster zunächst davon ausgegangen, dass den Beschäftigten die private Internetnutzung (welche auch die Nutzung von Webmail-Diensten, wie z. B. web.de, gmx.net, umfasst) gestattet wird, eine private Nutzung des betrieblichen E-Mail-Accounts jedoch verboten ist.
- Die Musterbetriebsvereinbarung behandelt ausschließlich datenschutzrechtliche Aspekte; ggf. sind darüber hinaus arbeitsrechtliche Fragestellungen zu beachten.

Dieses Muster kann auch für den Erlass einer Richtlinie/Anweisung oder als Orientierung für im Arbeitsvertrag zu regelnde Punkte herangezogen werden, wenn im Unternehmen kein Betriebsrat existiert. Ebenso kann die Orientierungshilfe analog im öffentlichen Bereich angewandt werden; hierbei sind landesspezifische Vorschriften zu beachten.

Betriebsvereinbarung[6]

Zwischen
der A-GmbH
und
dem Betriebsrat der A-GmbH
wird folgende Betriebsvereinbarung über die
"Nutzung von Internet und E-Mail"
geschlossen.
(Präambel)

1. Gegenstand und Geltungsbereich

1.1 Die Betriebsvereinbarung regelt die Grundsätze für die Nutzung der betrieblichen Kommunikationssysteme E-Mail und Internet.
1.2 Diese Betriebsvereinbarung gilt räumlich für den Betrieb der A-GmbH in ...
1.3 Die Betriebsvereinbarung gilt persönlich für Beschäftigte der A-GmbH.

2. Betriebliche und/oder private Nutzung

Die Nutzung der von der Arbeitgeberin zur Verfügung gestellten Kommunikationssysteme und Endgeräte zur Nutzung von Internet ist grundsätzlich

nur zu betrieblichen Zwecken gestattet. Das betriebliche E-Mail-Postfach darf <u>ausschließlich zur betrieblichen Kommunikation</u> genutzt werden.

2.1 Die Gestattung der privaten Nutzung des Internetzugangs nach den Vorgaben dieser Betriebsvereinbarung erfolgt ausschließlich gegenüber denjenigen Beschäftigten, die zuvor gegenüber der Arbeitgeberin eine Einwilligung gemäß **Anlage 1** abgegeben haben.

2.2 Liegt eine Einwilligung vor, ist die private Nutzung des betrieblichen Internetzugangs im Umfang von [*Definition durch Vertragspartner*] zulässig.

2.3 Die Beschäftigten sind frei in ihrer Entscheidung, ob sie eine solche Einwilligung abgeben wollen. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerruflich. Soweit die Einwilligung nicht erteilt wird oder widerrufen wurde, so ist nur eine betriebliche Nutzung zulässig.

3. Verhaltensgrundsätze

3.1 Unzulässig ist jede vorsätzliche Nutzung der betrieblichen Kommunikationssysteme, die den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit schadet oder die gegen geltende Rechtsvorschriften verstößt. Dazu zählen

- der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
- das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder
- Aktivitäten, die sich gegen das Unternehmen richten (sog. Compliance-Verstöße [*von Vertragspartnern zu konkretisieren*])
- ...

3.2 *[Hinweise, soweit bestimmte Internetseiten/-dienste gesperrt werden (blacklists)]*

3.3 Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen ist der Download von Programmen aus dem Internet nicht gestattet.

4. Nutzungsregelungen und Zugriffsrechte

4.1 [*ggf. allgemeine Regelungen zum Herunterladen von Inhalten, Speicherungen von Anhängen/Dateien, Möglichkeit bzw. Pflicht zur Verschlüsselung von E-Mails etc.*]

4.2 Bei geplanter Abwesenheit eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten sowie auf seine Vertretung einzurichten. Soweit dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

4.3 a) Wurde eine Abwesenheitsnachricht entgegen 4.2 nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.
b) Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insbesondere soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.
c) Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Beschäftigten für betriebliche Zwecke – etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden – darf darüber hinaus nur erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

Derartige Zugriffe können unter Hinzuziehung von Vertrauenspersonen [*konkret zu benennen*] im Vier-Augen-Prinzip durchgeführt werden. Der Beschäftigte wird über den Zugriff unverzüglich unterrichtet. Erkennbar private E-Mails und solche, die der Kommunikation des Beschäftigten mit den unter 4.6 angesprochenen Stellen dienen, dürfen inhaltlich nicht zur Kenntnis genommen werden.

4.4 Die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs werden zur Sicherstellung der Funktionsfähigkeit des Systems im Abstand von ... Tagen gespeichert und für maximal ... Jahre aufbewahrt.

4.5 Um gesetzlich vorgegebenen Aufbewahrungspflichten (z. B. gemäß § 257 HGB, § 147 AO) gerecht zu werden, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs im Abstand von ... Tagen archiviert und für maximal ... Jahre aufbewahrt.

4.6 Persönliche, aber geschäftlich veranlasste E-Mails (z. B. Kommunikation mit Betriebsrat, Betriebsarzt, Sozialberatung, Datenschutz oder Compliance Office) sollten über alternative Kommunikationswege abgewickelt werden (z. B. telefonisch, postalisch, private E-Mail-Adresse). Sollte dennoch derlei Kommunikation über das betriebliche E-Mail-Postfach abgewickelt werden, ist diese zu löschen bzw. lokal abzuspeichern. Bei einem Zugriff erkannte derartige Kommunikation (z. B. anhand des Betreffs bzw. Kommunikationspartners) darf inhaltlich nur durch den vorgesehenen Empfänger zur Kenntnis genommen werden.

5. Funktionspostfächer

E-Mail-Postfächer und die Internetkommunikation von Personen, die einer besonderen Vertraulichkeit unterliegen, sind von den Kontrollen nach dieser Vereinbarung ausgeschlossen. Eine Aufstellung dieser Postfächer findet sich in **Anlage 2**.

6. Spamfilter und Virenschutz

6.1 Durch eine zentrale Spamfilterung können Spammails erkannt werden, indem auf eingehende E-Mails zugegriffen wird. Erkannte Spammails werden im Betreff mit dem Wort „Spam“ markiert und an den Empfänger weitergeleitet. Dieser hat sorgfältig zu prüfen, inwieweit es sich tatsächlich um eine Spam-Nachricht handelt. Ist dies zutreffend, sollte diese unverzüglich gelöscht werden und der Erhalt derartiger E-Mails möglichst unterbunden werden.

6.2 Liegen konkrete Anhaltspunkte dafür vor, dass eine E-Mail Schadsoftware enthält, so wird diese automatisiert herausgefiltert und untersucht. Bestätigt sich der Verdacht, findet eine Weiterleitung an den Empfänger nur statt, wenn zuvor die entsprechenden Teilinhalte oder Anlagen entfernt wurden und Störungen oder Schäden durch die Weiterleitung ausgeschlossen werden können.

7. Verhaltenskontrolle

Die bei der Nutzung des betrieblichen E-Mail-Postfachs und des Internets anfallenden personenbezogenen Daten werden nur im Rahmen dieser Betriebsvereinbarung kontrolliert; insofern findet eine Verhaltenskontrolle statt. Sie unterliegt der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften. Darüber hinausgehende Leistungs- und Verhaltenskontrollen werden nicht durchgeführt.

8. Protokollierung

8.1 Die Nutzung des Internets wird, soweit dies für die Gewährleistung der Systemsicherheit und/oder der Funktionsfähigkeit der eingesetzten IT-Systeme erforderlich ist, mit folgenden Informationen für jedes aufgerufene Objekt protokolliert:

- Datum/Uhrzeit
- Benutzerkennung
- IP-Adresse
- Zieladresse
- übertragene Datenmenge
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.2 Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Message-ID
- Nachrichtengröße
- Betreff
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.3 Die Protokolldaten nach Ziffer 8.1 und 8.2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Aktualisierung der Liste gesperrter Internetseiten („Blacklist“)
- Optimierung des Netzes und
- Datenschutzkontrolle

verwendet.

8.4 Die Protokolldaten nach Ziffer 8.1 werden für maximal ...[7] Tage, Protokolldaten nach Ziffer 8.2 werden für maximal ... Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert. Die Regelungen zur Zweckbindung aus § 31 des Bundesdatenschutzgesetzes sind zu beachten.

8.5 Personal, das Zugang zu Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet. Bei der Auswahl des Personals ist dies als Eignungsvoraussetzung zu berücksichtigen. Dafür wird auch (z. B. durch vertragliche Vereinbarung) Sorge getragen, wenn und soweit es sich nicht um eigenes Personal handelt.

9. Kontrollen

9.1 Zur Aktualisierung der gesperrten Internetseiten (Blacklist) und zur Analyse von

- deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten oder
- extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externer E-Mail-Domänen

kann die geschäftliche und private Nutzung von Internet und E-Mail mit folgenden Kontrolldaten für einen Zeitraum von einem Monat protokolliert und getrennt von den Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 gespeichert werden:

- Gruppenzugehörigkeit,[8]
- Datum und Uhrzeit,
- genutzte externer E-Mail-Domänen,
- aufgerufene Internetdomänen (URLs),
- übertragene Datenmengen.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domänanalysen). Diese anonymen Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

9.2 Ergeben sich bei der Auswertung der Daten nach Ziffer 9.1 Hinweise auf unzulässige Zugriffe gemäß Ziffer 3.1 oder auf eine Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren stattfinden kann. An der Festlegung des Verfahrens der Auswertung von Protokolldaten sind der Betriebsrat, die IT-Abteilung und der betriebliche Datenschutzbeauftragte zu beteiligen. Das Verfahren ist den Beschäftigten bekannt zu geben.

9.3 Für die gezielte Kontrolle (personenbezogene Auswertung) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang der Daten, der Zeitraum der Auswertung vorab in einem Konzept festgelegt und angekündigt werden; der Umfang der von der Auswertung erfassten Personen muss dabei auf den Kreis der nach § 32 Abs. 1 Satz 2 BDSG Betroffenen begrenzt werden. Es dürfen nicht sämtliche Beschäftigte überwacht werden. Die personenbezogenen Daten sind nach Beendigung des Verfahrens zu löschen. Über das Ergebnis der Auswertung wird der Beschäftigte schriftlich in Kenntnis gesetzt. Ihm ist Gelegenheit zur Stellungnahme zu geben. Entsprechend den Ergebnissen der Auswertung ist das weitere Vorgehen (Stufe 4) abzuwägen:

- Einstellen der Kontrollen/keine weitere Überwachung,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
- Verschärfen der Kontrolle, indem die Protokollierung auf dem Arbeitsplatzrechner stattfindet.

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bleibt hiervon unberührt.

9.4 Für die Protokollierung auf dem Arbeitsplatzrechner (Stufe 4) gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Beschäftigten müssen über diese Maßnahme nachträglich aufgeklärt werden.

9.5 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 über einen Zeitraum bis zu maximal ... Tagen aufzubewahren und personenbezogen auszuwerten.

Erweist sich der Verdacht als unbegründet oder werden die Protokolldateien nicht mehr zu weitergehenden Maßnahmen nach Ziffer 8 dieser Vereinbarung benötigt, so hat die Stelle, die eine Speicherung der Protokolldaten über ... Tage hinaus veranlasst hat, unverzüglich die Löschung dieser Daten durch die IT-Abteilung zu veranlassen. Die erfolgte Löschung ist schriftlich gegenüber der beauftragenden

Stelle durch die IT-Abteilung zu bestätigen. Die Betroffenen werden nach Abschluss der Maßnahmen unverzüglich darüber benachrichtigt.

9.6 Ein Verstoß gegen diese Betriebsvereinbarung kann arbeitsrechtliche Konsequenzen haben.

Darüber hinaus kann ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen, z.B. bei Nutzung kostenpflichtiger Internetseiten.

Die Arbeitgeberin behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs und des betrieblichen E-Mail-Postfachs im Einzelfall zu untersagen.

10. Schulung der Beschäftigten

Die Beschäftigten werden in regelmäßig stattfindenden Schulungen mit den technischen Möglichkeiten und einer datenschutzgerechten Anwendung der eingesetzten Verfahren vertraut gemacht. Gleichzeitig werden sie über Art und Umfang der Erhebung und Verwendung ihrer personenbezogenen Daten informiert.

11. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten rechtzeitig mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden. Zur Evaluierung dieser Betriebsvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

12. Schlussbestimmungen

12.1 Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden Betriebsrat und Arbeitgeberin unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

12.2 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist ... gekündigt werden.

12.3 Im Falle einer Kündigung dieser Betriebsvereinbarung gelten diese Regelungen bis zum Abschluss einer neuen Vereinbarung. Nach Eingang der Kündigung verpflichten sich die Betriebsparteien, unverzüglich Verhandlungen über eine neue Betriebsvereinbarung aufzunehmen.

Anlagen:

- Anlage 1: Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetes
- Anlage 2: Von den Kontrollen ausgenommene E-Mail-Postfächer

Ort, den xx.xx.xxxx	Ort, den xx.xx.xxxx
______________________________	____________________________________
A-GmbH	Betriebsrat der A-GmbH

Anlage 1 zur Musterbetriebsvereinbarung (Anhang 1): Einwilligungserklärung

Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetzugangs

Ich möchte von dem Angebot Gebrauch machen, den betrieblichen Internetzugang in geringfügigem Umfang [*konkret bestimmen*] auch für private Zwecke zu nutzen.

1. Ich habe die Gelegenheit gehabt, die Betriebsvereinbarung über die Nutzung von Internet und E-Mail zur Kenntnis zu nehmen, und bin mir über die folgenden, mit der Privatnutzung des Internets verbundenen Nutzungsbedingungen bewusst:

- Die private Nutzung ist nur in geringfügigem Umfang [*konkret bestimmen*] gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.
- Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.
- Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen der Arbeitgeberin oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere
  - der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
  - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
  - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver), oder
  - Aktivitäten, die sich gegen das Unternehmen richten (z. B. Compliance-Verstöße [*konkret benennen*])
  - [... *an Regelung in Betriebsvereinbarung anpassen*]

  ist unzulässig.

- Die A-GmbH ist berechtigt, den Aufruf bestimmter Internetseiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internetinhalte.

2. Ich willige ein, dass auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe im Rahmen der Betriebsvereinbarung vom [*Datum einsetzen*] verarbeitet und unter den Voraussetzungen der Ziffern 8. und 9. der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden.

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gemäß § 88 TKG verzichte.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs das Internet nicht mehr privat nutzen darf.

Ort, Datum

____

Unterschrift des Beschäftigten

____

Anlage 2 zur Musterbetriebsvereinbarung (Anhang 1): Ausgenommene E-Mail-Postfächer

Von den Kontrollen ausgenommene E-Mail-Postfächer

Aufgrund gesetzlicher Verschwiegenheitsverpflichtungen von den Kontrollen ausgenommene E-Mail-Postfächer/-Funktionspostfächer:

- Betriebsarzt:
- Betriebsrat:
- Datenschutzbeauftragter:
- usw.

Anhang 2:

Muster einer Betriebsvereinbarung für die private Nutzung des Internets und des betrieblichen E-Mail-Postfachs

Hinweise:

- Entsprechend der Darstellung unter C.II. wird im folgenden Muster davon ausgegangen, dass den Beschäftigten die private Nutzung des Internets und des betrieblichen E-Mail-Postfachs gestattet wird.
- Die Musterbetriebsvereinbarung behandelt ausschließlich datenschutzrechtliche Aspekte; ggf. sind darüber hinaus arbeitsrechtliche Fragestellungen zu beachten.

Dieses Muster kann auch für den Erlass einer Richtlinie/Anweisung oder als Orientierung für im Arbeitsvertrag zu regelnde Punkte herangezogen werden, wenn im Unternehmen kein Betriebsrat existiert. Ebenso kann die Orientierungshilfe analog im öffentlichen Bereich angewandt werden; hierbei sind landesspezifische Vorschriften zu beachten.

Betriebsvereinbarung[9]

Zwischen
der A-GmbH
und
dem Betriebsrat der A-GmbH
wird folgende Betriebsvereinbarung über die
"Nutzung von Internet und E-Mail"
geschlossen.
(Präambel)

1. Gegenstand und Geltungsbereich

1.1 Die Betriebsvereinbarung regelt die Grundsätze für die Nutzung der betrieblichen Kommunikationssysteme E-Mail und Internet.

1.2 Diese Betriebsvereinbarung gilt räumlich für den Betrieb der A-GmbH in ...

1.3 Die Betriebsvereinbarung gilt persönlich für Beschäftigte der A-GmbH.

2. Betriebliche und/oder private Nutzung

Die Nutzung der von der Arbeitgeberin zur Verfügung gestellten Kommunikationssysteme und Endgeräte zur Nutzung von E-Mail und Internet ist grundsätzlich nur zu betrieblichen Zwecken gestattet.

2.1 Die Gestattung der privaten Nutzung des Internetzugangs und des betrieblichen E-Mail-Postfachs nach den Vorgaben dieser Betriebsvereinbarung erfolgt ausschließlich gegenüber denjenigen Beschäftigten, die zuvor gegenüber der Arbeitgeberin eine Einwilligung gemäß **Anlage 1** abgegeben haben.

2.2 Liegt eine Einwilligung vor, ist die private Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Postfachs im Umfang von [*Definition durch Vertragspartner*] zulässig.

2.3 Die Beschäftigten sind frei in ihrer Entscheidung, ob sie eine solche Einwilligung abgeben wollen. Die Einwilligung ist jederzeit mit Wirkung für die Zukunft widerruflich. Soweit die Einwilligung nicht erteilt wird oder widerrufen wurde, so ist nur eine betriebliche Nutzung zulässig.

3. Verhaltensgrundsätze

3.1 Unzulässig ist jede vorsätzliche Nutzung der betrieblichen Kommunikationssysteme, die den Interessen des Arbeitgebers oder dessen Ansehen in der Öffentlichkeit schadet oder die gegen geltende Rechtsvorschriften verstößt. Dazu zählen

- der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
- das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver) oder
- Aktivitäten, die sich gegen das Unternehmen richten (sog. Compliance-Verstöße [*von Vertragspartnern zu konkretisieren*])
- ...

3.2 *[Hinweise, soweit bestimmte Internetseiten/-dienste gesperrt werden (blacklists)]*

3.3 Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen ist der Download von Programmen aus dem Internet nicht gestattet.

4. Nutzungsregelungen und Zugriffsrechte

4.1 [*ggf. allgemeine Regelungen zum Herunterladen von Inhalten, Speicherungen von Anhängen/Dateien, Möglichkeit bzw. Pflicht zur Verschlüsselung von E-Mails etc.*] Gesendete und empfangene private E-Mails sind in einen Ordner „Privates“ zu verschieben bzw. zu löschen.

4.2 Bei geplanter Abwesenheit eines Beschäftigten ist durch den Beschäftigten ein automatisierter Hinweis auf die Abwesenheit des Beschäftigten sowie auf seine Vertretung einzurichten. Soweit dies für betriebliche Zwecke erforderlich ist, kann ein Vertretungsassistent eingerichtet werden bzw. können eingehende E-Mails automatisiert an einen Vertreter weitergeleitet werden.

4.3 a) Wurde eine Abwesenheitsnachricht entgegen 4.2 nicht eingerichtet oder war dies aufgrund einer ungeplanten Abwesenheit nicht möglich, kann dies durch den Arbeitgeber erfolgen.
b) Eine automatisierte Weiterleitung wird nur in dringend erforderlichen Fällen eingerichtet, insbesondere soweit eine Abwesenheitsnachricht allein den betrieblichen Erfordernissen nicht gerecht wird.
c) Ein Zugriff auf das betriebliche E-Mail-Postfach des betroffenen Beschäftigten für betriebliche Zwecke – etwa wenn Inhalte des Postfachs für die weitere Bearbeitung benötigt werden – darf darüber hinaus nur erfolgen, soweit dies für betriebliche Zwecke erforderlich ist.

Derartige Zugriffe können unter Hinzuziehung von Vertrauenspersonen [*konkret zu benennen*] im Vier-Augen-Prinzip durchgeführt werden. Der Beschäftigte wird über den Zugriff unverzüglich unterrichtet. Erkennbar private E-Mails und solche, die der Kommunikation des Beschäftigten mit den unter 4.7 angesprochenen Stellen dienen, dürfen inhaltlich nicht zur Kenntnis genommen werden.

4.4 Vor seinem Ausscheiden hat der Beschäftigte seine privaten Mails bzw. den Ordner „Privates“ aus dem betrieblichen E-Mail-Postfach zu entfernen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen]* **einzuräumen.**

4.5 Die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs werden zur Sicherstellung der Funktionsfähigkeit des Systems im Abstand von ... Tagen gespeichert und für maximal ... Jahre aufbewahrt. Davon können bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs auch private E-Mails betroffen sein, soweit sie nicht vor der Speicherung gelöscht bzw. in einen als „persönlich“ gekennzeichneten Ordner abgelegt wurden. Solche E-Mails werden nicht für den genannten Zweck gespeichert. Vor seinem Ausscheiden hat der Beschäftigte seinen persönlichen Ordner zu löschen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen*] **einzuräumen.**

4.6 Um gesetzlich vorgegebenen Aufbewahrungspflichten (z. B. gemäß § 257 HGB, § 147 AO) gerecht zu werden, werden die eingehenden und ausgehenden E-Mails des betrieblichen E-Mail-Postfachs im Abstand von ... Tagen archiviert und für maximal ... Jahre aufbewahrt. Davon können bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs auch private E-Mails betroffen sein, soweit sie nicht vor der Archivierung gelöscht bzw. in einen als „persönlich“ gekennzeichneten Ordner abgelegt wurden. Vor seinem Ausscheiden hat der Beschäftigte seinen persönlichen Ordner zu löschen. **Ihm ist dazu eine angemessene Zeit** [*konkret festzulegen*] **einzuräumen.**

4.7 Persönliche, aber geschäftlich veranlasste E-Mails (z. B. Kommunikation mit Betriebsrat, Betriebsarzt, Sozialberatung, Datenschutz oder Compliance Office) sollten über alternative Kommunikationswege abgewickelt werden (z. B. telefonisch, postalisch, private E-Mail-Adresse). Sollte dennoch derlei Kommunikation über das betriebliche E-Mail-Postfach abgewickelt werden, ist diese zu löschen bzw. lokal abzuspeichern. Bei einem Zugriff erkannte derartige Kommunikation (z. B. anhand des Betreffs bzw. Kommunikationspartners) darf inhaltlich nur durch den vorgesehenen Empfänger zur Kenntnis genommen werden.

5. Funktionspostfächer

E-Mail-Postfächer und die Internetkommunikation von Personen, die einer besonderen Vertraulichkeit unterliegen, sind von den Kontrollen nach dieser Vereinbarung ausgeschlossen. Eine Aufstellung dieser Postfächer findet sich in **Anlage 2**.

6. Spamfilter und Virenschutz

6.1 Durch eine zentrale Spam-Filterung können Spam-Mails erkannt werden, indem auf eingehende E-Mails zugegriffen wird. Bei erlaubter Privatnutzung des betrieblichen E-Mail-Postfachs wird auch auf den Betreff und den Inhalt privater E-Mails zugegriffen. Erkannte Spam-Mails werden im Betreff mit dem Wort „Spam“ markiert und an den Empfänger weitergeleitet. Dieser hat sorgfältig zu prüfen, inwieweit es sich tatsächlich um eine Spam-Nachricht handelt. Ist dies zutreffend, sollte diese unverzüglich gelöscht werden und der Erhalt derartiger E-Mails möglichst unterbunden werden.

6.2 Liegen konkrete Anhaltspunkte dafür vor, dass eine E-Mail Schadsoftware enthält, so wird diese automatisiert herausgefiltert und untersucht. Bestätigt sich der Verdacht, findet eine Weiterleitung an den Empfänger nur statt, wenn zuvor die entsprechenden Teilinhalte oder Anlagen entfernt wurden und Störungen oder Schäden durch die Weiterleitung ausgeschlossen werden können.

7. Verhaltenskontrolle

Die bei der Nutzung des betrieblichen E-Mail-Postfachs und des Internets anfallenden personenbezogenen Daten werden nur im Rahmen dieser Betriebsvereinbarung kontrolliert; insofern findet eine Verhaltenskontrolle statt. Sie unterliegt der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften. Darüber hinausgehende Leistungs- und Verhaltenskontrollen werden nicht durchgeführt.

8. Protokollierung

8.1 Die Nutzung des Internets wird, soweit dies für die Gewährleistung der Systemsicherheit und/oder der Funktionsfähigkeit der eingesetzten IT-Systeme erforderlich ist, mit folgenden Informationen für jedes aufgerufene Objekt protokolliert:

- Datum/Uhrzeit
- Benutzerkennung
- IP-Adresse
- Zieladresse
- übertragene Datenmenge
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.2 Ein- und ausgehende E-Mails werden mit folgenden Informationen protokolliert:

- Datum/Uhrzeit
- Absender- und Empfängeradresse
- Message-ID
- Nachrichtengröße
- Betreff
- ... [*abschließende Aufzählung aller Protokolldaten*]

8.3 Die Protokolldaten nach Ziffer 8.1 und 8.2 werden ausschließlich zu Zwecken der

- Analyse und Korrektur technischer Fehler,
- Gewährleistung der Systemsicherheit,
- Aktualisierung der Liste gesperrter Internetseiten („blacklist“),
- Optimierung des Netzes und
- Datenschutzkontrolle

verwendet.

8.4 Die Protokolldaten nach Ziffer 8.1 werden für maximal ...[10] Tage, Protokolldaten nach Ziffer 8.2 werden für maximal ... Tage aufbewahrt und dann automatisch gelöscht oder wirksam anonymisiert. Die Regelungen zur Zweckbindung aus § 31 des Bundesdatenschutzgesetzes sind zu beachten.

8.5 Personal, das Zugang zu Protokollinformationen hat, wird besonders auf die Sensibilität dieser Daten hingewiesen und auf die Einhaltung des Datenschutzes verpflichtet. Bei der Auswahl des Personals ist dies als Eignungsvoraussetzung zu berücksichtigen. Dafür wird auch (z. B. durch vertragliche Vereinbarung) Sorge getragen, wenn und soweit es sich nicht um eigenes Personal handelt.

9. Kontrollen

9.1 Zur Aktualisierung der gesperrten Internetseiten (blacklist) und zur Analyse von

- deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten oder
- extensivem Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externer E-Mail-Domänen

kann die geschäftliche und private Nutzung von Internet und E-Mail mit folgenden Kontrolldaten für einen Zeitraum von einem Monat protokolliert und getrennt von den Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 gespeichert werden:

- Gruppenzugehörigkeit,[11]
- Datum und Uhrzeit,
- genutzte externe E-Mail-Domänen,
- aufgerufene Internetdomänen (URLs),
- übertragene Datenmengen.

Für die Analysen werden statistische Aufbereitungen der protokollierten Kontrolldaten angefertigt, indem die im Zeitraum der Protokollierung auffällig häufig aufgerufenen Domänen und Übertragungsvolumina für Internet und E-Mail dargestellt sind (Domänanalysen). Diese Kontrolldaten werden durch den Arbeitgeber monatlich oder aus gegebenem Anlass gesichtet und ausgewertet.

9.2 Ergeben sich bei der Auswertung der Daten nach Ziffer 9.1 Hinweise auf unzulässige Zugriffe gemäß Ziffer 3.1 oder auf eine Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren stattfinden kann. An der Festlegung des Verfahrens der Auswertung von Protokolldaten sind der Betriebsrat, die IT-Abteilung und der betriebliche Datenschutzbeauftragte zu beteiligen. Das Verfahren ist den Beschäftigten bekannt zu geben.

9.3 Für die gezielte Kontrolle (personenbezogene Auswertung) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang der Daten, der Zeitraum der Auswertung vorab in einem Konzept festgelegt und angekündigt werden; der Umfang der von der Auswertung erfassten Personen muss dabei auf den Kreis der nach § 32 Abs. 1 Satz 2 BDSG Betroffenen begrenzt werden. Es dürfen nicht sämtliche Beschäftigte überwacht werden. Die personenbezogenen Daten sind nach Beendigung des Verfahrens zu löschen. Über das Ergebnis der Auswertung wird der Beschäftigte schriftlich in Kenntnis gesetzt. Ihm ist Gelegenheit zur Stellungnahme zu geben. Entsprechend den Ergebnissen der Auswertung ist das weitere Vorgehen (Stufe 4) abzuwägen:

- Einstellen der Kontrollen/keine weitere Überwachung,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
- Verschärfen der Kontrolle, indem die Protokollierung auf dem Arbeitsplatzrechner stattfindet.

Die Durchführung weiterer arbeitsrechtlicher Maßnahmen bleibt hiervon unberührt.

9.4 Für die Protokollierung auf dem Arbeitsplatzrechner (Stufe 4) gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Beschäftigten müssen über diese Maßnahme nachträglich aufgeklärt werden.

9.5 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts bei der Internet- oder E-Mail-Nutzung Protokolldaten nach Ziffer 8.1 und Ziffer 8.2 über einen Zeitraum bis zu maximal ... Tagen aufzubewahren und personenbezogen auszuwerten.

Erweist sich der Verdacht als unbegründet oder werden die Protokolldateien nicht mehr zu weitergehenden Maßnahmen nach Ziffer 8 dieser Vereinbarung benötigt, so hat die Stelle, die eine Speicherung der Protokolldaten über ... Tage hinaus veranlasst hat, unverzüglich die Löschung dieser Daten durch die IT-Abteilung zu veranlassen. Die erfolgte Löschung ist schriftlich gegenüber der beauftragenden Stelle durch die IT-Abteilung zu bestätigen. Die Betroffenen werden nach Abschluss der Maßnahmen unverzüglich darüber benachrichtigt.

9.6 Der Arbeitgeber ist berechtigt, bei Vorliegen eines auf zu dokumentierende tatsächliche Anhaltspunkte begründeten Missbrauchsverdachts(u. a. Compliance-Verstoß) bei der Nutzung des betrieblichen E-Mail-Postfachs unter Beteiligung des Datenschutzbeauftragten im Vier-Augen-Prinzip Zugriff auf die gespeicherten E-Mails zu nehmen [Anmerkungen: Ausführungen zu konkretem Verfahren: u. a. was unter einem Compliance-Verstoß zu verstehen ist, Verfahren selbst, beteiligte Personen, Dokumentation des Zugriffs und Informationen des betroffenen Beschäftigten].

9.7 Ein Verstoß gegen diese Betriebsvereinbarung kann arbeitsrechtliche Konsequenzen haben.

Darüber hinaus kann ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen, z. B. bei Nutzung kostenpflichtiger Internetseiten.

Die Arbeitgeberin behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs und des betrieblichen E-Mail-Postfachs im Einzelfall zu untersagen.

10. Schulung der Beschäftigten

Die Beschäftigten werden in regelmäßig stattfindenden Schulungen mit den technischen Möglichkeiten und einer datenschutzgerechten Anwendung der eingesetzten Verfahren vertraut gemacht. Gleichzeitig werden sie über Art und Umfang der Erhebung und Verwendung ihrer personenbezogenen Daten informiert.

11. Änderungen und Erweiterungen

Geplante Änderungen und Erweiterungen an den elektronischen Kommunikationssystemen werden dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten rechtzeitig mitgeteilt. Es wird dann geprüft, ob und inwieweit sie sich auf die Regelungen dieser Vereinbarung auswirken. Notwendige Änderungen oder Erweiterungen zu dieser Vereinbarung können im Einvernehmen in einer ergänzenden Regelung vorgenommen werden. Zur Evaluierung dieser Betriebsvereinbarung ist nach Ablauf von zwei Jahren ein Erfahrungsbericht vorzulegen.

12. Schlussbestimmungen

12.1 Die Unwirksamkeit einzelner Bestimmungen dieser Vereinbarung führt nicht zur Unwirksamkeit der übrigen Regelungen. Im Falle der Unwirksamkeit einzelner Regelungen werden Betriebsrat und Arbeitgeberin unverzüglich Verhandlungen über eine Neuregelung des jeweiligen Sachverhalts aufnehmen.

12.2 Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist ... gekündigt werden.

12.3 Im Falle einer Kündigung dieser Betriebsvereinbarung gelten diese Regelungen bis zum Abschluss einer neuen Vereinbarung. Nach Eingang der Kündigung verpflichten sich die Betriebsparteien, unverzüglich Verhandlungen über eine neue Betriebsvereinbarung aufzunehmen.

Anlagen:

- Anlage 1:
  Einwilligungserklärung zur privaten Nutzung des betrieblichen Internets und des betrieblichen E-Mail-Postfachs
- Anlage 2:
  Von den Kontrollen ausgenommene E-Mail-Postfächer

Ort, den xx.xx.xxxx	Ort, den xx.xx.xxxx
______________________________	______________________________
A-GmbH	Betriebsrat der A-GmbH

Anlage 1 zur Musterbetriebsvereinbarung (Anhang 2): Einwilligungserklärung

Einwilligungserklärung zur privaten Nutzung des betrieblichen Internetzugangs und des betrieblichen E-Mail-Postfachs

Ich möchte von dem Angebot Gebrauch machen, den betrieblichen Internetzugang und das betriebliche E-Mail-Postfach in geringfügigem Umfang [konkret bestimmen] auch für private Zwecke zu nutzen.

1. Ich habe die Gelegenheit gehabt, die Betriebsvereinbarung über die Nutzung von Internet und E-Mail zur Kenntnis zu nehmen, und bin mir über die folgenden, mit der Privatnutzung des Internets und des betrieblichen E-Mail-Postfachs verbundenen Nutzungsbedingungen bewusst:
    - Die private Nutzung ist nur in geringfügigem Umfang [konkret bestimmen] gestattet und nur sofern und soweit dadurch die geschäftliche Aufgabenerfüllung und die Verfügbarkeit der IT-Systeme für geschäftliche Zwecke nicht beeinträchtigt werden.
    - Zum Schutz der IT-Systeme vor Viren, Trojanern und ähnlichen Bedrohungen sind der Download von Programmen aus dem Internet sowie entsprechende Downloads von Dateianhängen im Rahmen der privaten Nutzung nicht gestattet.
    - Eine vorsätzliche Nutzung, welche geeignet ist, den Interessen der Arbeitgeberin oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Rechtsvorschriften verstößt, insbesondere
        - der Abruf von für den Arbeitgeber kostenpflichtigen Internetseiten,
        - das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
        - Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z. B. Angriffe auf externe Webserver), oder
        - Aktivitäten, die sich gegen das Unternehmen richten (z.B. Compliance-Verstöße [konkret benennen])
        - [... *an Regelung in Betriebsvereinbarung anpassen*]

      ist unzulässig.

    - Die A-GmbH ist berechtigt, den Aufruf bestimmter Internetseiten durch den Einsatz geeigneter Filter-Programme zu verhindern. Es besteht kein Rechtsanspruch auf einen Zugriff auf gefilterte Internetinhalte.

2. **Ich willige ein, dass**
    - **auch meine privaten – also nicht nur die betrieblichen – Internetzugriffe und meine private E-Mail-Kommunikation im Rahmen dieser Betriebsvereinbarung verarbeitet und unter den Voraussetzungen der Ziffern 8. und 9. der Betriebsvereinbarung protokolliert sowie personenbezogen ausgewertet werden,**
    - **bei einer Abwesenheit meinerseits, entsprechend der Ziffer 4.3 der Betriebsvereinbarung, ein Zugriff für betriebliche Zwecke auf mein betriebliches E-Mail-Postfach erfolgen darf und auch ein Hinweis auf meine Abwesenheit hinterlegt wird oder in dringend erforderlichen Fällen eine Weiterleitung auf das E-Mail-Postfach meines Vertreters eingerichtet wird bzw. ein Zugriff des Arbeitgebers auf mein E-Mail-Postfach ermöglicht wird,**
    - **eine Speicherung meiner privaten E-Mails im Rahmen der Sicherstellung der IT-Sicherheit des Systems erfolgt, sofern ich diese nicht vor dem Zeitpunkt der Speicherung gelöscht bzw. in meinen Ordner „Privates“ verschoben habe,**
    - **eine Archivierung meiner privaten E-Mails erfolgt, sofern ich diese nicht vor dem Zeitpunkt der Archivierung gelöscht bzw. in meinen Ordner „Privates“ verschoben habe.**

Im Rahmen einer gezielten Kontrolle nach Ziffer 9.2 wünsche ich die Einbeziehung folgender Vertrauenspersonen:

____

Mir ist bewusst, dass ich hierdurch auf den Schutz des Fernmeldegeheimnisses gemäß § 88 TKG verzichte. Mir ist weiter bekannt, dass bei der zentralen Spam-Filterung automatisch auf den Betreff oder Inhalte auch meiner privaten E-Mails zugegriffen wird. Mir ist auch bewusst, dass ich vor meinem Ausscheiden aus dem Unternehmen alle privaten E-Mails und meinen Ordner „Privates“ löschen muss.

Ich bin mir darüber im Klaren, dass eine missbräuchliche oder unerlaubte Nutzung neben arbeitsrechtlichen Konsequenzen gegebenenfalls auch strafrechtliche Folgen haben kann und dass darüber hinaus ein Verstoß zivilrechtliche Schadensersatzpflichten auslösen kann.

Mir ist bewusst, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, mit der Folge, dass ich ab dem Zeitpunkt des Widerrufs den Internetzugang und das betriebliche E-Mail-Postfach nicht mehr privat nutzen darf.

Ort, Datum Unterschrift des Beschäftigten

Anlage 2 zur Musterbetriebsvereinbarung (Anhang 2): Ausgenommene E-Mail-Postfächer

Von den Kontrollen ausgenommene E-Mail-Postfächer

Aufgrund gesetzlicher Verschwiegenheitsverpflichtungen von den Kontrollen ausgenommene E-Mail-Postfächer / Funktionspostfächer:

- Betriebsarzt:
- Betriebsrat:
- Datenschutzbeauftragter:
- usw.

---

[1] Aus Gründen der Übersichtlichkeit wird im Folgenden ausschließlich von der Betriebsvereinbarung gesprochen. Gemeint ist jedoch auch die Anweisung/Richtlinie oder eine Regelung im Arbeitsvertrag.

[2] Hessischer VGH, 19.05.2009, AZ: 6 A 2672/08.Z; LAG Niedersachsen, 31.05.2010, AZ: 12 Sa 875/09; LAG Berlin-Brandenburg, 16.02.2011, AZ: 4 Sa 2132/10; VG Karlsruhe, 27.05.2013, AZ: 2 K 3249/12; VGH Baden-Württemberg, 30.07.2014, 1 S 1352/2013. Die genannten Gerichte haben zudem zum Teil die Auffassung vertreten, dass der Schutz des Fernmeldegeheimnisses jedenfalls in dem Moment endet, in dem der Empfänger in der Weise Zugriff auf die E-Mails in seinem betrieblichen E-Mail-Postfach hat, dass er entscheiden kann, ob er sie im zentralen Posteingang belässt oder auf einen lokalen Rechner verschiebt/löscht.

[3] Zum Umfang von Stichproben wird auf die arbeitsrechtliche Rechtsprechung, insbesondere BAG, Beschluss vom 09.07.2013 - 1 ABR 2/13 (A), verwiesen.

[4] Siehe A II 1.

[5] Siehe A II 1.

[6] Die Musterbetriebsvereinbarung stellt eine Empfehlung der Datenschutzaufsichtsbehörden dar. Sie ist den konkreten Gegebenheiten im Unternehmen anzupassen. Abweichungen sind möglich.

[7] Die Speicherdauer ist je nach den Umständen des Einzelfalls auf das erforderliche Maß zu begrenzen. In der Praxis der Aufsichtsbehörden hat sich dabei eine Frist von wenigen Tagen als in der Regel ausreichend herausgestellt. Der Grundsatz der Datensparsamkeit ist zu beachten. Von den Möglichkeiten zur Anonymisierung und/oder Pseudonymisierung ist zum frühestmöglichen Zeitpunkt Gebrauch zu machen. Protokolldateien zu Zwecken der Gewährleistung der Datensicherheit sind regelmäßig auszuwerten.

[8] Zur Eingrenzung des Personenkreises bei missbräuchlicher Nutzung können gruppenbezogen Nutzungsdaten erhoben werden. Eine Gruppe sollte mindestens so viele Mitarbeiter enthalten, dass keine Identifizierung droht.

[9] Die Musterbetriebsvereinbarung stellt eine Empfehlung der Datenschutzaufsichtsbehörden dar. Sie ist den konkreten Gegebenheiten im Unternehmen anzupassen. Abweichungen sind möglich.

[10] Die Speicherdauer ist je nach den Umständen des Einzelfalls auf das erforderliche Maß zu begrenzen. In der Praxis der Aufsichtsbehörden hat sich dabei eine Frist von wenigen Tagen als in der Regel ausreichend herausgestellt. Der Grundsatz der Datensparsamkeit ist zu beachten. Von den Möglichkeiten zur Anonymisierung und/oder Pseudonymisierung ist zum frühestmöglichen Zeitpunkt Gebrauch zu machen. Protokolldateien zu Zwecken der Gewährleistung der Datensicherheit sind regelmäßig auszuwerten.

[11] Zur Eingrenzung des Personenkreises bei missbräuchlicher Nutzung können gruppenbezogen Nutzungsdaten erhoben werden. Eine Gruppe sollte mindestens so viele Mitarbeiter enthalten, dass keine Identifizierung droht.

10.2

Orientierungshilfe[1] der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht

Stand: 07.04.2016

1. Zielsetzung

Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Zu diesen Zwecken werden auch an Schulen zunehmend Online-Lernplattformen für den Unterricht eingesetzt. Diese Online-Lernplattformen werden von Schulaufsichtsbehörden, Schulbuchverlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Die Vorteile werden in der orts- und zeitunabhängigen Nutzung dieser Verfahren gesehen. Allerdings werden dabei zahlreiche Schüler[2]- und Lehrerdaten webbasiert verarbeitet. Die vorliegende Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen (Mindest-)Kriterien Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Online-Lernplattformen sollen den Bildungs- und Erziehungsauftrag der Schule unterstützen, beispielsweise

- Kompetenzorientierung,
- Integration fachlicher, methodischer und sozialer Lernziele,
- Prozesshaftigkeit des Lerngeschehens,
- Unterstützung von Schülern in Kleingruppen,
- begabungsgerechte Förderung,
- Erkennen individueller Lernfortschritte und Lernschwierigkeiten,
- Beratung und Lernförderung einzelner Schüler.

Ergänzend wird auf die Orientierungshilfe der Arbeitskreise Technik und Medien der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises in der aktuellen Fassung verwiesen, weil diese besondere Anforderungen für webbasierte Anwendungen bzw. „Datenverarbeitung in der Wolke“ aufzeigt.

Soweit die Online-Lernplattformen für andere als schulische Zwecke über das Internet zur Nutzung zur Verfügung stehen, gelten darüber hinaus die Vorschriften des Telemediengesetzes[3] und des Telekommunikationsgesetzes. Sie sind jedoch nicht Gegenstand dieser Orientierungshilfe.

2. Begriffsbestimmungen

Online-Lernplattformen im Sinne dieser Orientierungshilfe sind Softwaresysteme, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation von Lerninhalten ergänzen oder sogar ersetzen. Schulsoftwaresysteme, die für Aufgaben der Schulverwaltung genutzt werden, sind davon systemtechnisch zu trennen.

Die virtuelle Lernumgebung einer Online-Lernplattform kann von der Schule so gestaltet werden, dass Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen eingerichtet werden.

Leistungsbewertungen haben einen erhöhten Schutzbedarf. Dieser ist durch entsprechende technisch-organisatorische Maßnahmen abzusichern.

Der Zugriff auf die Software erfolgt ortsunabhängig mittels eines Endgerätes (PC, Tablet etc.) über einen Web-Browser. Die faktische Teilhabe der Schüler ist durch die Schule zu gewährleisten. Jeder Teilnehmer an einem bestimmten Kurs, also z. B. die Schüler einer Klasse oder eines Jahrgangs in einem bestimmten Schulfach, muss sich vor einer Nutzung zunächst im Onlineverfahren auf der Lernplattform anmelden oder angemeldet werden. Das System stellt dann jedem Nutzer ein personalisiertes Benutzerkonto zur Verfügung. Darüber hinaus muss die Schule bzw. die verantwortliche Lehrkraft die Zugriffsrechte für die einzelnen Nutzer festlegen und die Funktionalitäten auswählen, die die Online-Lernplattform bietet (Bereitstellung von Lerninhalten, Diskussionsforen, Übungsaufgaben etc.).

3. Datenschutzrechtliche Problematik

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt werden.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist, und sind daher entsprechend anzupassen.

Auch beim Einsatz von Online-Lernplattformen benötigen Lehrkräfte die Möglichkeit, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wie oft und zu welchen Zeiten ein Schüler sich in der Online-Lernplattform an bestimmten Aufgaben beteiligt hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Die Schüler und – falls erforderlich – auch die Erziehungsberechtigten sind vor der Nutzung der Online-Lernplattform darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten haben kann.

Fazit:

- Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.
- Es bietet sich die Nutzung von Online-Lernplattformen an, die je nach vorgesehenem Einsatzszenario modular angepasst werden können.
- Die Betroffenen sind vor der Nutzung der Online-Lernplattform über mögliche Auswertungen umfassend zu informieren.

4. Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernplattformen sind zunächst die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen. Ergänzend können – je nach Bundesland und Schultyp – die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz zur Anwendung kommen.

Die verpflichtende Verwendung einer Lernplattform kann nur durch oder aufgrund eines Gesetzes vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung. Andernfalls kann es nur auf Basis einer freiwillig erteilten Einwilligung[4] zum Einsatz einer derartigen Plattform kommen.

Fazit:

Vor dem Einsatz der Online-Lernplattform ist zu prüfen, ob deren Einsatz rechtlich zulässig ist und ob die Schüler und ggf. die Erziehungsberechtigten in die Nutzung der Plattform einwilligen müssen.

5. Verantwortliche Stelle

Bei der Nutzung von Lernplattformen bleibt die Schule – oder je nach Bundesland die Schulaufsichtsbehörde – verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus, dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten“ bleibt. Lehrende dürfen im Rahmen der Freiheit der Gestaltung des Unterrichts nur insoweit Lernplattformen im Unterricht einsetzen, wie die Schule oder die Schulaufsicht über den Einsatz der jeweiligen Lernplattform entschieden hat.

6. Umfang der Datenverarbeitung

6.1 Erforderliche Daten

Die Schule/Schulaufsichtsbehörde muss festlegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden.

6.1.1 Zwingend erforderliche Stammdaten

- Name und Anschrift der jeweiligen Schule und der verantwortlichen Stelle, die, wenn die Schulaufsichtsbehörde diese Aufgaben wahrnimmt, differieren können.

– Stammdaten zur Anlage von Benutzerkonten, die sowohl zur Identifikation des Nutzers im System als auch zum Zwecke der Vergabe von Rollen und Berechtigungen dienen. Es gibt die Möglichkeit, dass der Nutzer selbst die Daten eingibt und anlegt oder dass die Daten durch die Schule erfasst oder geändert werden. Wichtig ist, dass nur Daten eingegeben werden können, die für die sinnvolle Nutzung der pädagogischen Aufgabenerfüllung der Schule erforderlich sind.

– Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Benutzernamen und dem Anmeldenamen zu unterscheiden. Der Benutzername muss den realen Namen (Klarname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch betreuende Lehrer erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmeldename wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Im Gegenteil: Die Nutzung von Pseudonymen als Anmeldenamen erhöht die Sicherheit im Vergleich zur Nutzung des Klarnamens. Der Anmeldename kann frei gewählt werden. Es wird die Anmeldung mit Pseudonymen empfohlen, um den Missbrauch des Kontos durch Dritte maßgeblich zu erschweren.

– Die Angabe einer E-Mail-Adresse ist je nach System optional oder zwingend erforderlich. Sie dient insbesondere der Zusendung von Benachrichtigungen aus den belegten Kursen sowie der Abfrage eines neuen Passworts bei dessen Verlust.

Ein Benutzerkonto kann weitere Informationen enthalten, die die Kommunikation innerhalb des Systems erleichtern, beispielsweise Klassenstufe, Bezeichnung der Lerngruppe, Ausbildungsgang (beispielsweise an berufsbildenden Schulen).

Fazit:

– Bei der Auswahl der Online-Lernplattform ist darauf zu achten, dass die Grundsätze der Datensparsamkeit und Datenvermeidung (z. B. nicht zu viele Stammdaten, Freitextfelder, Kommentarfunktionen) gewährleistet werden.
– Es ist eine pseudonymisierte Nutzerverwaltung der Lernplattform anzustreben.

6.1.2 Optionale Daten

Weitere optionale Daten können im Nutzerprofil auf freiwilliger Basis durch den Benutzer selbst erfasst werden. Bei missbräuchlicher Nutzung einzelner Informationen (beispielsweise im Zusammenhang mit Mobbing) sollten die betreffenden Felder für alle Benutzerkonten deaktiviert werden. Felder wie „Beschreibung“, „Nutzerbild" und „Interessenfelder" verdienen in diesem Zusammenhang besonderes Augenmerk.

Optionale Datenfelder können bei den gängigen Online-Lernplattformen sein:

Zeitzone: Dieses Feld wird im Regelfall deaktiviert oder mit einem Standardwert belegt, da alle Nutzer in der Regel in der gleichen Zeitzone leben.
Beschreibung: Hier können Nutzer Angaben zur eigenen Person eintragen. Diese sind innerhalb der Lernplattform, nicht aber öffentlich sichtbar. Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
Nutzerbild: Der Nutzer kann eine Grafikdatei (beispielsweise ein Porträtfoto) hochladen, für die er die Urheberrechte besitzt. Dieses Feld ist nicht erforderlich, birgt die Gefahr von Rechtsverstößen und sollte deaktiviert werden.
Interessenfelder: Hier können Schlagworte zur eigenen Person angegeben werden (beispielsweise Hobbys). Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
Webseite: Teilnehmer können hier die URL zu einer eigenen Internetpräsenz angeben. Dieses Feld ist zu deaktivieren.
Bevorzugte Sprache: Die Einstellung ermöglicht, dass Benutzeroberflächen in anderen Sprachen als Deutsch zur Verfügung stehen. Dieses Feld ist in aller Regel nicht erforderlich und sollte deaktiviert werden.
Institution, Abteilung: Diese Information wird in der Regel in der Schule nicht verwandt.

Für organisatorische Zwecke können zusätzliche optionale Datenfelder angelegt und gepflegt werden. Dies ist nur zulässig, soweit es für die Aufgabenerfüllung erforderlich ist. Zu denken ist hier beispielsweise an die Angabe, an welchen Kursen ein Schüler teilnimmt, damit er Zugang zu den zugehörigen Dokumenten erhält. Nicht hierunter fallen persönliche Angaben wie Hobbys oder private Telefonnummern.

6.1.3 Nutzungsdaten

Bei der Nutzung einer Lernplattform werden automatisch Daten über den Nutzer und seine Aktivitäten erfasst und gespeichert. Diese Logdaten werden auf dem Server abgelegt, sie dürfen ausschließlich für die Überwachung der Funktionsfähigkeit und Sicherheit dieser Systeme sowie bei rechtswidrigem Missbrauch verwendet werden. Ergänzend wird auf die Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder in der aktuellen Fassung verwiesen. Näheres sollte in der Nutzungsordnung konkret festgelegt werden.

Nutzungsdaten sind in aller Regel für die Wahrnehmung schulischer Aufgaben nicht erforderlich und sollten daher nur unter klar definierten Voraussetzungen für eindeutig bestimmte Personengruppen zu festgelegten Zwecken einsehbar sein. Nutzungsdaten sind beispielsweise

- Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung
- Protokollierung von Eingaben oder Änderungen
- IP-Adressen, genutzte Dienste (z. B. Dateidownloads, Chat)

6.1.4 Pädagogische Prozessdaten

Als pädagogische Prozessdaten werden Informationen bezeichnet, die dem Lehrer die Möglichkeit geben, den individuellen und kollektiven Lernprozess nachzuvollziehen, um didaktische Interventionen zu planen, Unterricht zu reflektieren, zu evaluieren und weiterzuentwickeln sowie individuelle Lernberatung für einzelne Schüler oder kleine Gruppen zu gestalten. In den verschiedenen Modulen einer Online-Lernplattform werden Prozessdaten generiert, die jeweils für unterschiedliche Personenkreise sichtbar sind. Solche Module sind:

- Forendiskussion: Die Beiträge können den Verfassern zugeordnet und in zeitlicher Struktur geordnet werden. Zudem zeigt die Darstellungsstruktur an, zu welchem Beitrag eine Antwort abgegeben wurde. Diese Informationen sind für alle Nutzer sichtbar. Eine Anzeige noch nicht gelesener Beiträge hingegen ist nur für den jeweiligen Einzelnutzer sichtbar.

- Wiki-Einträge: Ein Wiki ist ein mehrseitiges Dokument, an dem von verschiedenen Verfassern in einem Kurs gearbeitet wird. Durch die Speicherung der Historie ist erkennbar, wer welche Teile an einem Dokument bearbeitet hat. Die Lehrkraft kann dadurch die Beteiligung und die Beiträge Einzelner erkennen. Dies ist für Rückmeldungen und die Bewertung sowie die Förderung sozialer und kommunikativer Aspekte des Lernens wichtig.

- Glossar (Datenbank): Das Glossar stellt eine Sammlung von Informationen in strukturierter Form dar. Es enthält einzelne Texteinträge mit Angaben zum Erstellungszeitpunkt und dem Verfasser. Diese Details sind für alle Nutzer sichtbar.

- Lernobjekte (Aufgaben, Tests): Je nach Art des Objekts sind unterschiedliche Daten nur für Lehrkräfte oder auch für einzelne Schüler sichtbar. Eine Überwachung der außerunterrichtlichen Aktivitäten von Schülern durch Lehrende darf nicht stattfinden. Die Sichtbarkeit der Daten für Lehrende ist pädagogisch zu begründen und von der Schulleitung bzw. der Schulkonferenz festzulegen.

- SCORM-Module, LTI-Module, Live Classroom, Plagiatsüberprüfung etc.: Bei der Nutzung derartiger Module werden unter Umständen personenbezogene Daten an externe Dienstleister weitergegeben. Dies ist nur im Rahmen von bestehenden Auftragsdatenverarbeitungsverträgen zwischen Schule/Schulträger und Anbieter zulässig und ist datenschutzrechtlich gesondert zu prüfen. Prozessdaten von Lernenden dürfen nur dann für andere Teilnehmer sichtbar sein, wenn dies methodisch oder didaktisch erforderlich ist. Als Beispiel sei die Bewertungsfunktion in einem Diskussionsforum angeführt. Je nach Implementierung erlaubt sie eine schnelle, unter Umständen nonverbale Rückmeldung zu Beiträgen. Da auf diese Weise von Schülern auch unsachgemäße und verletzende Kritik gegenüber Mitschülern geäußert werden kann, ohne dass von Seiten der Lehrenden rechtzeitig eingegriffen werden kann, ist eine solche Funktion nur mit Bedacht zu aktivieren.

6.1.5 Statistische Daten

Die Lernplattformen erlauben die Auswertung statistischer Daten beispielsweise über Art und Umfang der Nutzung. Echte statistische Daten haben aber keinen Personenbezug und sind daher aus datenschutzrechtlicher Sicht unproblematisch. Sollte es sich nicht um echte statistische Daten in diesem Sinne handeln, gelten für sie die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen der Länder.

6.2 Schriftliche Festlegungen

Vor dem Einsatz der Online-Lernplattform hat die Schule/die Schulaufsichtsbehörde schriftliche Festlegungen zur zulässigen Datennutzung und zum Rollen- und

Berechtigungskonzept zu treffen. Außerdem muss dies in das Verfahrensverzeichnis aufgenommen werden.

Die Vorgaben zur Konfiguration und Anwendung der Online-Lernplattform durch die Administratoren, Lehrer und Lehrerinnen kann beispielsweise in Form einer Nutzerordnung geschehen, in der klar geregelt wird, wie die Vertraulichkeit, Integrität, Authentizität, die Nichtverkettbarkeit der Daten und die Intervenierbarkeit des Nutzers entsprechend dem jeweils geltenden Landesrecht vor Ort konkret umzusetzen ist. Hierzu gehören ein Löschkonzept (9.9) sowie die Frage, welche E-Mail-Adressen verwendet werden (9.2).

Fazit:

Die Grundlagen der Datenverarbeitungsprozesse sind vor dem Einsatz der Online-Lernplattform abschließend in einer Nutzerordnung festzulegen.

7. Notwendige Prüfungen vor Inbetriebnahme

Vor dem Einsatz von Lernplattformen hat die verantwortliche Stelle (Schule oder Schulaufsichtsbehörde) im Zusammenwirken mit ihrem Datenschutzbeauftragten eine Vorabkontrolle nach den jeweils geltenden Landesregelungen durchzuführen. Hierbei sind insbesondere folgende Aspekte zu beachten:

- Einhaltung der ggf. bestehenden landesrechtlichen Regelungen zum Einsatz von Online-Lernplattformen
- Bei der Anschaffung einer Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser die datenschutzrechtlichen schulischen Anforderungen erfüllen kann.
- Gestaltung und Auswahl von Datenverarbeitungssystemen nach den Grundsätzen der Datenvermeidung und Datensparsamkeit
- Beim Einsatz von externen Dienstleistern sind die gesetzlichen Voraussetzungen der zulässigen Auftragsdatenverarbeitung zu beachten. Dabei gelten folgende allgemeine Anforderungen:
    - Die Schule/Schulaufsichtsbehörde muss „Herrin der Daten“ bleiben. Sie bestimmt, wer die Daten auf welche Weise verarbeitet und nutzt. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht in Bezug auf die Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen lassen.
    - Die Allgemeinen Geschäftsbedingungen externer Dienstleister sind unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern.
    - Mit dem Auftragnehmer ist ein Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung genügt.
- Es gilt der Grundsatz der Zweckbindung. Danach ist insbesondere zu gewährleisten, dass die Daten der Schüler, Lehrer und Eltern nicht zu Werbezwecken genutzt werden.
- Die von der Schule/Schulaufsichtsbehörde zu erstellenden Nutzungsbedingungen, das Verfahrensverzeichnis und die sonstigen getroffenen technischen und organisatorischen Maßnahmen sind einer datenschutzrechtlichen Prüfung zu unterziehen.

8. Unterrichtungs-, Benachrichtigungs-, Schulungs- und Unterweisungspflichten

Schüler, Eltern[5] und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten. Sie sind darüber aufzuklären, dass sie jederzeit berechtigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht und dessen Rechtsfolgen zu informieren. Die Einwilligung ist schriftlich einzuholen. Aus der Einwilligung hat hervorzugehen, welche Daten in welcher Form und zu welchem Zweck verarbeitet werden sollen. Darüber hinaus sind die Nutzer darüber zu informieren, ob und an wen Daten übermittelt werden.

Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen.

9. Hinweise zur technischen und organisatorischen Umsetzung

9.1 Passwörter

Die Nutzung einer Online-Plattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen verschlüsselt gespeichert werden. Es muss gewährleistet sein, dass niemand innerhalb der Lernplattform Passwörter im Klartext einsehen kann. Dies gilt auch für Administratoren.

Bei der Vergabe von Passwörtern durch die Schule ist zu gewährleisten, dass bei der ersten Nutzung des Logins der Nutzer sein Passwort ändern muss. Von dieser Regel kann im begründeten Einzelfall abgewichen werden (beispielsweise bei Grundschülern oder Schülern mit speziellem Förderbedarf). Nutzer mit der administrativen Berechtigung zur Bearbeitung der Benutzerkonten im System können für andere Nutzer Passwörter zurücksetzen. Von der Vergabe neuer Passwörter wird abgeraten, da dann der Administrator Kenntnis vom neuen Passwort erlangt. Bei der Passwortgenerierung, dem Passwortgebrauch und der Passwortverwaltung sollte die Maßnahme „2.11 – Regelung des Passwortgebrauchs“ der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge beachtet werden. Dies betrifft insbesondere die Komplexität des Passwortes und die Geheimhaltungspflicht. Die Passwörter sind nach spätestens 90 Tagen gemäß M 2.11 zu wechseln.

Für die Verwendung von Passwörtern muss eine Vorgabe erfolgen, die die Mindestzahl an Zeichen und deren Zusammensetzung (Zahl der Großbuchstaben, Zahl der Kleinbuchstaben, Zahl der Ziffern und Zahl der Sonderzeichen) festlegt. Bei der Festlegung dieser Vorgaben ist das Alter der Schüler zu beachten, um keine Zugangsprobleme zu schaffen. Ein Passwort soll aber in keinem Falle kürzer als acht Zeichen sein.

9.2 E-Mail-Adresse

Die E-Mail-Adresse ist ein eindeutiger Wert. Soll eine E-Mail-Adresse innerhalb der Lernplattform zur Verfügung gestellt werden, dann ist sicherzustellen, dass diese E-Mail-Adresse nicht für mehrere Benutzerkonten verwendet werden kann. Die Verwendung der E-Mail-Adressen ist schriftlich zu regeln.

9.3 Erfassung der Daten des Benutzerkontos und Änderbarkeit

Benutzerkonten können durch Import, manuelle Eingabe oder Anbindung an eine bestehende Datenbank nach Maßgabe der in der Schule verwandten Systeme angelegt werden. Bei einem Import oder einer Anbindung an eine bestehende Datenbank sollte nur der Anmeldename, wie er im bestehenden Datenbestand gespeichert ist, an die Lernplattform übermittelt werden (unidirektionaler Informationsfluss). Das Passwort muss den Richtlinien aus 9.1 entsprechen und daher evtl. neu vergeben werden. Die Schule oder die Schulaufsichtsbehörde legt die Vorgehensweise in Form von einer Nutzerordnung fest.

9.4 Öffentliche Bereiche

Es ist grundsätzlich möglich, bestimmte Bereiche einer Online-Lernplattform öffentlich zugänglich zu machen. Für diese Bereiche gelten dieselben datenschutzrechtlichen Regelungen wie für andere Internetpräsenzen von Schulen, insbesondere im Hinblick auf die Nennung von Namen oder die Abbildung von Schülern oder Lehrkräften; darüber hinaus gelten das Telemediengesetz und das Telekommunikationsgesetz. Unter Beachtung der einschlägigen Vorschriften muss eine allgemeine Zugänglichkeit immer unterbleiben, sobald dadurch personenbezogene Daten sichtbar werden.

9.5 Suchmaschinen

Bereiche, in denen nutzerspezifische Daten gespeichert werden, dürfen nicht öffentlich angeboten werden. Es ist dafür Sorge zu tragen, dass öffentliche Suchmaschinen (Google, Bing etc.) keinen Zugriff auf diese Bereiche haben.

9.6 Rollenkonzept

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden.

Folgende Grundsätze sind bei der Vergabe von Rechten und Rollen zu beachten:

Ein **Administrator** kann auf alle Bereiche zugreifen. Personen mit Administrationsberechtigungen können daher alle Kurse sowie alle Beiträge der Schüler und Lehrer einsehen. Dies schließt Bewertungen mit ein. Bei der Vergabe von Administrationsrechten muss daher mit besonderer Sorgfalt vorgegangen werden, und zwar:

- Jedem Administrator ist ein eigener personenbezogener Benutzeraccount zuzuweisen, d. h., es ist nicht zulässig, dass mehrere Administratoren das gleiche Benutzerkonto (= Gruppenadministratorkonto) nutzen. Der Anmeldename des Administrators muss pseudonym sein, um so eine missbräuchliche Kontosperrung zu verhindern. Das Pseudonym muss so gewählt werden, dass es nicht auf einfachem Weg herauszufinden ist.
- Administratoren, die gleichzeitig noch andere Tätigkeiten wahrnehmen, wie z. B. auch Lehraufgaben, müssen über ein separates Benutzerkonto für diese Zwecke verfügen. Es muss also die Möglichkeit bestehen, einer Person entsprechend ihren verschiedenen Rollen mehrere Benutzerkonten zuweisen zu können.
- Die Anzahl der Administratorenkonten ist so gering wie möglich zu halten, um das Missbrauchsrisiko zu minimieren (z. B. unbefugte Kenntnisnahme, unkontrollierbare Rechtevergaben etc.). Eine Vertretungsregelung muss aber gewährleistet sein.
- Administratorenrechte darf nur erhalten, wer innerhalb des Systems entsprechende Aufgaben tatsächlich wahrnehmen muss.
- Alle Aktivitäten der Administratoren sind ausschließlich zu Zwecken der Datenschutzkontrolle für einen Zeitraum von maximal einem Jahr zu protokollieren.

9.7 Zugriffsrechte

9.7.1 Zugriff durch schulinterne Stellen oder Personen

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schriftlich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

Mitglieder der Schulleitung und gegebenenfalls Funktionsträger haben das Recht zur Durchführung von Unterrichtshospitationen. Dieses Recht dient der Wahrnehmung der Führungsaufgabe, der Beschaffung von Informationen und Eindrücken zur Unterrichts- und Schulkonzeptentwicklung. In vielen Schulen werden Klassenarbeiten exemplarisch nach der Bewertung und vor der Rückgabe an die Schüler der Schulleitung zur Information und Kenntnisnahme vorgelegt. Gleichwohl dürfen diese Zugriffe nur erfolgen, soweit es für die jeweilige Aufgabe erforderlich ist.

Werden Online-Lernplattformen eingesetzt, so werden sie automatisch zu einem Bestandteil der Unterrichtsarbeit. Damit gelten die schulinternen Vereinbarungen, die im Hinblick auf Hospitationen getroffen wurden, auch hier.

Die Art der Einsichtnahme der Schulleitung in die Arbeit mit einer Online-Lernplattform muss den schulinternen Vereinbarungen entsprechen, wie sie für Unterrichtshospitationen im Klassenraum gelten. Die Nutzer der Lernplattform sind über diese Vorgehensweisen und Vereinbarungen vor Beginn der Nutzung zu informieren. Jede Einsichtnahme wird in derselben Weise dokumentiert, wie dies für Hospitationen im regulären Unterrichtsbetrieb erforderlich und festgelegt ist.

Eine Überwachung der Arbeit mit der Lernplattform durch die Schulleitung oder andere Stellen und Personen ist nicht zulässig. Insbesondere darf auch eine Überwachung der Aktivitäten von Schülern durch Lehrende nicht stattfinden. Etwas anderes gilt, wenn die Plattform für pädagogische Aufgaben, wie organisierte Chats zu bestimmten Themen, Gruppenarbeiten usw. genutzt wird, die einer Benotung unterfallen. In diesem Fall darf die für die Benotung notwendig zu beobachtende Aktivität durch die Lehrkraft überwacht werden. Der Umfang der Daten, die für Lehrende sichtbar sein sollen, ist daher pädagogisch zu begründen und von der Schulkonferenz festzulegen. Ebenso wenig dürfen die Aktivitäten von Lehrenden durch Vorgesetzte auf der Online-Lernplattform überwacht werden. Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.7.2 Zugriff auf die Daten durch schulexterne Stellen oder Personen

Schulexterne haben grundsätzlich keinen Zugriff auf geschützte Bereiche der Online-Lernplattform. Sollte es in begründeten Ausnahmefällen nötig sein, so ist jeder Zugriff dieser Art zuvor durch die verantwortliche Stelle auf seine Rechtmäßigkeit zu prüfen. Die Teilnehmer sind über diesen Zugriff frühzeitig zu informieren. Es ist im Rahmen der datenschutzrechtlichen Vorschriften zulässig, externen Personen, die nicht als Lehrer, Schüler oder Mitarbeiter in der Schulverwaltung tätig sind, einen temporären und begrenzten

Zugriff auch auf geschützte Bereiche der Lernplattform zu geben, sofern dies für die Gewährleistung der Funktion des Systems erforderlich ist, beispielsweise bei einer Fernwartung. Hierbei muss mit dem jeweiligen Auftragnehmer ein Vertrag über die Auftragsdatenverarbeitung abgeschlossen werden.

9.8 Datenlöschung

Soweit die Speicherung personenbezogener Daten einer Einwilligung bedarf, werden die gespeicherten Daten der Lehrer und Schüler gelöscht, wenn die Einwilligung widerrufen wird. Die Daten der Schüler in Kursen (letzte Bearbeitung, bearbeitete Lektionen, Fehler, Korrekturanmerkungen u. Ä.) werden jeweils am Ende des laufenden Schuljahres gelöscht. Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen sind ebenfalls zu beachten. Es ist schriftlich festzulegen, wie die Aufbewahrungsfristen eingehalten werden. Ausnahmen sind zulässig beispielsweise bei schuljahresübergreifenden Projekten zur Vorbereitung auf Nachprüfungen, bei abiturrelevanten Kursen und aufgrund von Dokumentationspflichten der Schule. Auch E-Portfolios der Schüler können im Sinne einer Sicherheitskopie während der Zeit des kompletten Schulbesuchs hinterlegt werden. Die übrigen Daten der Schüler und Lehrer werden spätestens am Ende des Schuljahres gelöscht, in dem die Lehrkraft von der Schule abgegangen ist oder der Schüler ausgetreten ist.

Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen oder wenn diese ihre Einwilligung widerrufen.

Die unter 6.1.3 genannten Log-Daten (z. B. wann welcher Nutzer auf welche Daten zugegriffen hat oder wann welche Funktionen genutzt wurden) fallen auf Serverseite an und ermöglichen es, Probleme beim technischen Betrieb und beim Zugriff der Nutzer im Bedarfsfall zu untersuchen und zu lösen. Die Speicherdauer sollte maximal zehn Tage betragen. Eine längere Speicherdauer ist nur in begründeten Ausnahmefällen zulässig. Für weitergehende Regelungen zur Protokollierung wird auf die o. g. Orientierungshilfe „Protokollierung“ verwiesen.

Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

9.9 Trennung der Datenbanken

Jede Schule wird als eigenständige Organisationseinheit verstanden. Die Daten verschiedener Schulen sind logisch getrennt zu halten und zu verwalten. Es muss mindestens gewährleistet sein, dass Schulen nur auf ihre eigenen Daten zugreifen können. Hierzu wird auf die OH Mandantenfähigkeit des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der jeweils aktuellen Fassung verwiesen.

9.10 Sonstige technische Maßnahmen

Es sollten konkrete Maßnahmen vorgeschlagen werden, die insbesondere den Zugriff externer Stellen auf die Daten verhindern und gewährleisten, dass die Datenübertragung auf den häuslichen Rechner der Lehrkräfte und Schüler sowie je nach Rollenkonzept ggf. der Eltern sicher vor unbefugtem Zugriff erfolgt. Die jeweils zu treffenden Maßnahmen richten sich dabei nach den konkreten Umständen des Einzelfalls. Je nach der Art der betroffenen Daten, dem Personenkreis, der auf sie Zugriff haben soll, dem Ort, an dem die Daten gespeichert werden, differiert das Maß der erforderlichen Sicherheit. Wenn es sich lediglich um eine reine Lernplattform handelt, die nur Informationen für die Schüler zur Verfügung stellt, sind nicht die gleichen hohen Schutzmaßnahmen erforderlich wie bei einer Plattform, auf der Noten abgespeichert werden und auf die in bestimmten Bereichen auch Dritte Zugriff haben.

Die Sicherheitsmaßnahmen betreffen insbesondere drei Punkte: die Datensicherheit auf dem Server, den Schutz des Administratorzugangs und den Schutz der Datenübertragung hin zum Nutzer.

1. Auf dem Server sollten nur Hintergrundsysteme zur Datenspeicherung eingesetzt werden, welche eine automatische Zugriffsrechteverwaltung mitbringen, die durch die Lernplattform auch genutzt werden sollte, d. h., ein Default-Nutzer als einziger Datenzugriffsberechtigter ist nicht zulässig (hier wäre sonst der Datenbestand unter Kenntnis des Default-Nutzers komplett auslesbar). Vor Einsatz einer entsprechenden Lernplattform muss das Programm dahingehend geprüft werden, dass eine vollumfängliche Nutzerverwaltung stattfindet.

2. Der Administratorzugriff ist innerhalb der Lernplattform ein sehr kritischer Punkt. Das Passwort sollte gängigen Sicherheitsvorkehrungen genügen. Es wird hierbei auf die

jeweils aktuelle BSI-Richtlinie zur Erstellung von Passwörtern verwiesen. In Anbetracht der sehr experimentierfreudigen Natur der Schüler sollte außerdem die Administration nur über für Schüler unzugängliche Rechner erfolgen, da dann ausgeschlossen werden kann, dass Schüler unbemerkt Schadsoftware installieren können, die dann das Administratorpasswort ausspähen könnte. Außerdem ist der Einsatz einer Firewall und aktueller Anti-Viren-Software auf dem Server unerlässlich. Eine Zweifaktor-Authentisierung, wie sie bei vielen webbasierten Anwendungen Standard ist, wird für administrative Zugriffe bei Anwendungen mit erhöhtem Funktionsumfang (Tests, Hausaufgabenkontrolle etc.) empfohlen.

3. Die Datenübertragung zwischen Server und Nutzer ist zu verschlüsseln. Je nach Lernplattform ist dabei der Einsatz der Verschlüsselungstechnologie einzeln zu prüfen.

---

[1] beschlossen auf der 91. DSK am 06./07.04.2016 mit Gegenstimme des Bayrischen Landesbeauftragten für den Datenschutz

[2] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt ein.

[3] Die Ausnahme des § 11 Abs. 1 TMG greift in diesem Fall nicht.

[4] Es ist zu beachten, dass sich das Einwilligungserfordernis danach richtet, wie einsichtsfähig die Schüler sind. Die Erforderlichkeit der Einbeziehung der Eltern sollte mit dem zuständigen Landesbeauftragten für Datenschutz abgestimmt werden.

[5] Hier ist zu beachten, dass die Eltern möglicherweise bei volljährigen Schülern nach dem geltenden Landesrecht nicht immer eine Zugriffsberechtigung haben dürfen.

10.3

Datenschutzrechtliche Eckpunkte zu den in die Öffentlichkeit gelangten Überlegungen des BMI für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU)

Inhaltsverzeichnis

1. Vorbemerkung

In die Öffentlichkeit sind Überlegungen des BMI für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU – Stand: 5. August 2016) gelangt. In der Erwartung, dass diese nochmals eingehend überarbeitet werden, ist eine detaillierte Stellungnahme, insbesondere in Hinblick auf die Vereinbarkeit des DSAnpUG-EU mit der Datenschutz-Grundverordnung (DS-GVO), erst dann beabsichtigt, wenn ein belastbarer Entwurf vorliegt.

Die nachfolgenden generellen Erwägungen beschränken sich auf Art. 1 des DSAnpUG-EU im Zusammenhang mit der Umsetzung der DS-GVO. Sie sollen frühzeitig kommuniziert werden, um in die weitere Arbeit am Gesetzentwurf einfließen zu können. Materiellrechtliche Anmerkungen zu der Umsetzung der JI-Richtlinie enthält die Stellungnahme nicht.

2. Die Anmerkungen im Einzelnen

2.1 Allgemeine Hinweise

Eine klare Trennung zwischen der Umsetzung der Regelungsaufträge und -optionen nach der DS-GVO, der Umsetzung der JI-Richtlinie und der Regelung für die nicht unionsrechtlich erfassten Bereiche ist dringend erforderlich. Die Bezeichnung „Allgemeines Bundesdatenschutzgesetz“ (im Folgenden ABDSG-E) kann nicht überzeugen. Zudem sollte bei den einzelnen Paragraphen des ABDSG-E zwischen Regelungen für den öffentlichen und nicht-öffentlichen Bereich differenziert werden.

2.1.1 Klare Trennung zwischen der Umsetzung der Regelungsaufträge und -optionen nach der DS-GVO, der Umsetzung der JI-Richtlinie und der Regelung für die nicht unionsrechtlich erfassten Bereiche

Es ist schwierig, die Umsetzung der Richtlinie (EU) 2016/680 (JI-Richtlinie) gemeinsam mit der Anpassung des deutschen Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) vorzunehmen. Die Umsetzung dieses Regelungsansatzes führt in der Gesamtschau dazu, dass für den Rechtsanwender bei vielen Vorschriften deren Anwendungsbereich unklar bleibt. Einzelne Regelungen gelten nur im Anwendungsbereich der DS-GVO, andere nur im Zusammenhang mit der JI-Richtlinie und weitere nur für die nicht unionsrechtlich geregelten Bereiche. Daneben gibt es aber auch Bestimmungen, die für die vorgenannten Bereiche gemeinsam gelten sollen. Dies macht den Gesetzentwurf unübersichtlich und kaum handhabbar. Zur Gewährleistung des verfassungsrechtlichen Gebots der Normenklarheit sollten die unterschiedlichen Bereiche voneinander getrennt werden.

Rein vorsorglich wird darauf hingewiesen, dass die Umsetzung der JI-Richtlinie, insbesondere auch unter Berücksichtigung der Vorgaben des Bundesverfassungsgerichts, in dem bisherigen Entwurf der Vervollständigung bzw. Anpassung bedarf. Zudem muss die Regelung zum Inkrafttreten korrigiert werden. Das bisher vorgesehene Datum „25. Mai 2018“ entspricht den Vorgaben der DS-GVO, nicht aber den Vorgaben der JI-Richtlinie, die bestimmt, dass Umsetzungsvorschriften grundsätzlich bereits ab dem 6. Mai 2018 anzuwenden sind (vgl. Art. 63 Abs. 1 Satz 1 und 3 JI-RL). Eine detaillierte Stellungnahme für den Bereich der JI-Richtlinie ist vorgesehen.

2.1.2 Bezeichnung des Gesetzes in Art. 1 DSAnpUG-EU

Die Bezeichnung der Nachfolgeregelung des Bundesdatenschutzgesetzes als „allgemeines BDSG“ (ABDSG-E) ist nicht verständlich. In Abgrenzung zum allgemeinen Bundesdatenschutzgesetz gibt es kein besonderes Bundesdatenschutzgesetz, nur, wie bisher auch, bereichsspezifische Regelungen. Die Bezeichnung Bundesdatenschutzgesetz (BDSG) sollte beibehalten und Art. 1 als Änderungsgesetz zum BDSG ausgestaltet werden.

2.1.3 Einheitliche Verwendung der Begriffe der DS-GVO

Um eine einfache Anwendung und Auslegung des Gesetzes in Art. 1 DSAnpUG-EU (ABDSG-E) zu gewährleisten, sollte das Gesetz einheitlich die Begriffe der DS-GVO verwenden. Beispielsweise sollte statt der „Benennung einer oder eines Beauftragten für den Datenschutz“ in § 14 ABDSG-E entsprechend dem Wortlaut in Art. 37 DS-GVO die Formulierung „Benennung eines Datenschutzbeauftragten“ gewählt werden.

2.1.4 Deutliche Differenzierung zwischen den Regelungen für den öffentlichen und nicht-öffentlichen Bereich

Erhebliche Schwierigkeiten bereitet es, den Adressatenkreis der einzelnen Vorschriften des ABDSG-E aus sich heraus zu überblicken. Die Frage, ob die jeweilige Vorschrift für nicht-öffentliche Stellen, für öffentliche Stellen oder für beide gilt, kann vielfach erst durch Heranziehung der Gesetzesbegründung beantwortet werden.

Die fehlende Differenzierung zwischen dem öffentlichen und dem nicht-öffentlichen Bereich sollte insbesondere zur Zweckänderung und im Bereich der Einschränkung von Betroffenenrechten (Kapitel 3) überprüft werden. Der Umfang der Betroffenenrechte, wie er bislang im Bundesdatenschutzgesetz (BDSG) geregelt ist, soll nach dem Gesetzentwurf im Rahmen des europarechtlich Zulässigen weitestgehend in die §§ 7 ff. ABDSG-E überführt werden. Hierbei finden durch die gewählte „Vereinheitlichung“ Einschränkungen von Betroffenenrechten, die bislang nur für den nicht-öffentlichen Bereich konzipiert waren, nunmehr auch für den öffentlichen Bereich Anwendung. Im Hinblick auf die Grundsätze der Bestimmtheit, Lesbarkeit und Klarheit von Gesetzen sollte bezüglich jeder einzelnen Regelung des ABDSG-E deutlich gekennzeichnet werden, ob diese für öffentliche und bzw. oder nicht-öffentliche Stellen gilt. Dies darf sich nicht lediglich aus der Gesetzesbegründung, sondern muss sich bereits eindeutig aus dem jeweiligen Gesetzeswortlaut ergeben.

2.2 Bedenken hinsichtlich der Vereinbarkeit mit dem Grundgesetz und der DS-GVO

Zudem bestehen Bedenken hinsichtlich der Vereinbarkeit des ABDSG-E mit dem Grundgesetz und der DS-GVO. Die Regelungen sind oftmals zu unbestimmt und könnten Länderkompetenzen tangieren. Durch bloße Wiederholungen des Wortlautes der DS-GVO werden Öffnungsklauseln der DS-GVO, sofern diese überhaupt hinsichtlich einzelner Regelungen des ABDSG-E bestehen sollten, jedenfalls nicht ordnungsgemäß ausgefüllt.

2.2.1 Eingriff in die Gesetzgebungskompetenz der Länder

Trifft der Bundesgesetzgeber Regelungen zu den Aufsichtsbehörden der Länder, wie u. a. in §§ 16, 27, 29 ff. ABDSG-E geschehen, ist zwischen der BfDI und den Ländern umstritten, ob die Gesetzgebungskompetenz des Bundes gegeben ist. Während die Aufsichtsbehörden der Länder eine Zuweisung der primären Gesetzgebungskompetenz an die Länder sehen, hält die BfDI die sich aus der Begründung des Gesetzentwurfs ergebenden Erläuterungen zur Gesetzgebungskompetenz des Bundes für zutreffend.

2.2.2 Fehlerhafte Anwendung und Ausfüllung von Öffnungsklauseln der DS-GVO

Mit den Regelungen des ABDSG-E werden Regelungen getroffen, hinsichtlich derer teilweise keine Öffnungsklauseln in der DS-GVO zu Gunsten des nationalen Gesetzgebers bestehen.

Insbesondere Artikel 6 Abs. 4 der DS-GVO, auf den u. a. in § 6 ABDSG-E Bezug genommen wird, stellt keine generelle Ermächtigungsgrundlage für gesetzliche Regelungen im nicht-öffentlichen Bereich dar, sondern kommt nur dort zum Tragen, wo bereits Öffnungsklauseln zur Regelung der Erstverarbeitung existieren.

2.3 Materiellrechtliche Schwerpunkte

Zahlreiche Vorschriften im ABDSG-E lassen befürchten, dass mit dem DSAnpUG-EU datenschutzrechtliche Standards sinken. Die im ABDSG-E formulierten Regelungen zu den unabhängigen Datenschutzaufsichtsbehörden bedürfen zudem eingehender Überarbeitung. Die Vorschriften zum Beschäftigtendatenschutz und zum betrieblichen Datenschutzbeauftragten werden grundsätzlich begrüßt. Ergänzungen und Korrekturen werden für das Akkreditierungsverfahren, die Videoüberwachung und beim Scoring angeregt.

2.3.1 Drohende Absenkung des Datenschutzniveaus

Das ABDSG-E bleibt hinsichtlich des datenschutzrechtlichen Standards sowohl hinter dem bisherigen BDSG als auch der DS-GVO zurück. Noch in den Verhandlungen zur DS-GVO war es erklärtes Ziel, das hohe Datenschutzniveau in Deutschland keinesfalls preiszugeben. Während nunmehr die DS-GVO datenschutzfreundliche Innovationen bereithält, sucht der vorliegende Entwurf des DSAnpUG-EU den Datenschutzstandard in Deutschland, sowohl im Verhältnis zum Status quo als auch zur DS-GVO, deutlich abzusenken. Insbesondere für den nicht-öffentlichen Bereich werden Möglichkeiten geschaffen, die über das Erforderliche hinausgehen und das Recht auf informationelle Selbstbestimmung unangemessen einschränken. Die häufige Fokussierung auf die wirtschaftlichen Interessen geht zu Lasten des Persönlichkeitsschutzes und steht der Harmonisierung des Datenschutzrechts in Europa entgegen. Dies zeigt sich insbesondere darin, dass das ABDSG-E die Betroffenenrechte stärker einschränkt (vgl. §§ 7-11 ABDSG-E), als es nach der DS-GVO zulässig wäre, dass das in der DS-GVO angestrebte Maß an Transparenz wird verfehlt und die Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten (vgl. § 5 ABDSG-E) ausgeweitet werden. Die Ausweitung der Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten (vgl. § 5 ABDSG-E) und der in § 2 ABDSG an der Hauptniederlassung eines Unternehmens orientierte Anwendungsbereich des Gesetzes tragen ebenfalls dazu bei, dass das ABDSG-E die Ziele der DS-GVO verfehlt.

2.3.1.1 Einschränkung der Betroffenenrechte

Die Einschnitte in die Betroffenenrechte stellen lediglich eine Arbeitserleichterung für die datenverarbeitenden Stellen dar und stehen dem Schutzcharakter der Vorschriften zur Auskunft, Information und Löschung von Daten der DS-GVO diametral entgegen.

Artikel 23 DS-GVO erlaubt den Mitgliedstaaten, durch Rechtsvorschriften bestimmte Pflichten und Rechte der DS-GVO einzuschränken. Die Einschränkung muss eine zur Aufrechterhaltung der öffentlichen Sicherheit notwendige und verhältnismäßige Maßnahme darstellen (vgl. Erwägungsgrund 73). Die Schaffung einer Ausnahme von der Informationspflicht etwa bei „unverhältnismäßigem Aufwand“ entgegen Art. 13 DS-GVO (vgl. §§ 7 Abs. 2; 8 Abs. 2 lit. d; 10 Abs. 2), wegen der fehlenden Differenzierung sowohl im öffentlichen als auch nicht-öffentlichen Bereich, zeugt beispielhaft von dem unverhältnismäßigen Gebrauch der Einschränkungsmöglichkeit, der den Anforderungen von Art. 23 DS-GVO nicht genügt. Die verantwortliche Stelle vor hohem Verwaltungsaufwand zu bewahren, realisiert nicht den Schutz der Rechte und Freiheiten anderer Personen nach Art. 23 Abs. 1 lit. i DS-GVO. Die Vorschrift soll Dritte schützen und nicht den Verantwortlichen. Schon im Laufe des Gesetzgebungsverfahrens der DS-GVO scheiterte Deutschland mit der Forderung, einen unverhältnismäßigen Aufwand als Ausnahmetatbestand zu regeln. Entsprechend der Intention der DS-GVO haben die Verantwortlichen vielmehr durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, ihren Informations-, Auskunfts- und Löschpflichten zu genügen. Ebenso ist nicht ersichtlich, welchen in Art. 23 DS-GVO konkret genannten Zwecken die Einschränkung der Informationspflicht bei der Videoüberwachung in öffentlich zugänglichen Räumen (§ 7 Abs. 3 ABDSG) oder bei der Datenspeicherung zu Zwecken der Datensicherung und Datenschutzkontrolle (§ 8 Abs. 2 lit. d ABDSG-E) dienen sollten. Alle auf Art. 23 DS-GVO gestützten Einschränkungen bedürfen einer zwingenden Überprüfung, ob die Voraussetzungen des Art. 23 DS-GVO vorliegen, der Verhältnismäßigkeitsgrundsatz gewahrt ist und die jeweilige Formulierung von Ausnahmen dem Bestimmtheitsgrundsatz noch genügt. Außerdem sollten konkretere Regelungen zum Schutz der Rechte der Betroffenen in die einzelnen Bestimmungen des 3. Kapitels aufgenommen werden, beispielsweise dass eine Verwendung der Daten zu anderen Zwecken durch angemessene technische Maßnahmen ausgeschlossen ist, um zumindest einen Ausgleich zu den Beschränkungen der Information des Betroffenen zu erreichen.

2.3.1.2 Ausweitung der Befugnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten

Durch das ABDSG-E werden Befugnisse zur Datenverarbeitung gegenüber den Regelungen zur DS-GVO ausgeweitet. Dies zeigt sich insbesondere an der Aufgabe des grundsätzlichen Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten in § 5 ABDSG-E, der im Gegensatz zu Art. 9 DS-GVO nicht mehr als Ausnahmetatbestand formuliert ist.

Das Problem betrifft insbesondere Gesundheitsdaten (§ 4 Abs. 2 Nr. 10, 12, 15, § 5 Nr. 5, 7 ABDSG-E), biometrische Daten (§ 5 Abs. 1 Nr. 1 ABDSG-E) und die Verwendung besonderer Kategorien personenbezogener Daten im Beschäftigungsverhältnis (§ 5 Abs. 1 Nr. 6 ABDSG-E).

Die Anwendungsbereiche und das Verhältnis der einzelnen Normen bezüglich der Gesundheitsdaten zueinander sind unklar. § 4 ABDSG-E befasst sich mit der allgemeinen Zulässigkeit der Verarbeitung von personenbezogenen Daten durch öffentliche Stellen für die Wahrnehmung im öffentlichen Interesse liegender, nicht abschließend genannter Aufgaben, § 5 ABDSG-E mit der erforderlichen Verarbeitung besonderer personenbezogener Daten im abschließend genannten öffentlichen Interesse. In allen genannten Vorschriften sind Gesundheitsdaten betroffen. Eine Einschränkung der Person des Verarbeitenden erfolgt jedoch nur in § 4 Abs. 2 Nr. 10 und § 5 Nr. 4 ABDSG-E. In den anderen Fällen ist die Verarbeitung „ungeschützt“ zugelassen, im Falle von § 5 Nr. 7 ABDSG-E zumindest mit der Möglichkeit der Pseudonymisierung (§ 5 Abs. 1 S. 2 ABDSG-E).

Problematisch ist auch § 5 Abs. 1 Nr. 1 ABDSG-E, der die „Verarbeitung biometrischer Daten zu Zwecken der eindeutigen Identifikation betroffener Personen“ pauschal bereits als erhebliches öffentliches Interesse genügen lässt. Es wird weder zwischen Zwecken der Wirtschaft und staatlicher Aufgabenerfüllung unterschieden, noch wird zwischen unterschiedlichen biometrischen Verfahren differenziert. Die Formulierung stellt damit einen gefährlichen Freibrief für eine uferlose Verarbeitung biometrischer Daten zu Zwecken der eindeutigen Identifikation einer Person durch die Wirtschaft und durch staatliche Stellen aus. Gleiches zeigt sich etwa bei § 5 Abs. 1 Nr. 3 ABDSG, der den Wortlaut von § 13 Abs. 2 Nr. 6 BDSG jedoch ohne die Worte „zwingend erforderlich“ wiederholt. Die Ausnahmetatbestände müssen, sofern sie überhaupt Bestand haben können, als solche formuliert und gesondert für den öffentlichen und nicht-öffentlichen Bereich ausgewiesen werden.

Insbesondere im Arbeitsrecht ist aufgrund § 5 Abs. 1 Nr. 6 ABDSG-E mit einer erheblichen Ausweitung der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten zu rechnen. § 5 Abs. 1 Nr. 6 ABDSG-E stellt klar, dass besondere Kategorien personenbezogener Daten zur Wahrnehmung der aus dem Arbeitsrecht erwachsenden Rechte und Pflichten auch ohne Einwilligung der betroffenen Person (vgl. Artikel 9 Abs. 2 lit. b DS-GVO) verarbeitet werden dürfen. Das bringt zwar zunächst eine Erleichterung für den Arbeitgeber, soweit er Daten wie die Religionszugehörigkeit, gesundheitliche Eignung etc. für Zwecke des Arbeitsverhältnisses, etwa der Lohnabrechnung oder die Erfüllung seiner Fürsorgepflicht, verarbeitet. Allerdings besteht hier die Gefahr, dass besondere Kategorien personenbezogener Daten im Hinblick auf ihre Verarbeitung und Übermittlung, z. B. beim Datentransfer im Konzern, an Schutz verlieren. Zum „Arbeitsrecht“ gehören auch individualrechtliche Vereinbarungen und das kollektive Arbeitsrecht. Ob auch insoweit vereinbarte Rechte und Pflichten verhältnismäßig sind und die Interessen der Beschäftigten ausreichend berücksichtigen, ist eine Frage des Einzelfalls, kann aber nicht als Rechtsgrundlage für die Verarbeitung und Übermittlung von besonderen Kategorien personenbezogener Daten herangezogen werden.

Zu befürchten ist im Ergebnis, dass bei Beibehaltung des unspezifischen Begriffs „Arbeitsrecht“ lediglich aufgrund von einzelvertraglichen Vereinbarungen besondere Kategorien personenbezogener Daten in weltweiten Konzernstrukturen übermittelt werden. Klargestellt werden sollte daher, dass dies nur aufgrund von arbeitsrechtlichen Rechtsvorschriften, vor allem gesetzlichen Regelungen bzw. Betriebsvereinbarungen, möglich ist.

Im Übrigen sollte in § 5 Abs. 1 ABDSG-E zwischen öffentlichen Stellen und nicht-öffentlichen Stellen differenziert und § 5 Abs. 1 Satz 1 Nr. 4 ABDSG-E durch die konkretere Regelung des § 28 Abs. 7 BDSG ersetzt werden.

2.3.1.3 Fehlende Transparenz der Datenverarbeitung

Transparenz und transparente Informationen bilden einen zentralen Bestandteil in der DS-GVO. Die Einschnitte in die Betroffenenrechte durch das ABDSG-E sorgen für das Gegenteil: Eingriffe in die Datenschutzrechte der Betroffenen bleiben intransparent, sodass die Ausübung weiterer Rechte nach §§ 10 bis 13 ABDSG-E erschwert wird. Mangels nachträglicher Benachrichtigungspflichten scheitert auch eine durch den Betroffenen veranlasste Ex-post-Kontrolle durch die Aufsichtsbehörden. Dies zeigt sich beispielsweise in § 9 ABDSG-E. Dieser übernimmt in § 9 Abs. 2c ABDSG-E die bisherige Regelung nach § 34 Abs. 7 i. V. m. § 33 Abs. 2 S. 1 Nr. 2 BDSG, wonach eine Einschränkung des Auskunftsrechts der betroffenen Person dann besteht, wenn personenbezogene Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher bzw. vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen (also gesperrt werden müssen). Diese Regelung ist mit den Zielen der DS-GVO nicht mehr vereinbar. Die Erfahrung der Aufsichtsbehörden zeigt, dass Unternehmen in vielen Fällen ihrer Pflicht zur Sperrung dieser

Daten nicht nachkommen, was nicht selten zu einer (datenschutzwidrigen) zweckwidrigen Weiterverwendung führt. Diese bleibt jedoch dann unentdeckt, wenn die auskunftsersuchende betroffene Person nicht darüber informiert werden muss, dass (doch) Daten über sie gespeichert sind. Zur besseren Transparenz sollte das ABDSG-E ferner für die zuständige Aufsichtsbehörde eine ausdrückliche Befugnis enthalten, dem Betroffenen bestimmte Mitteilungen über das wesentliche Ergebnis der datenschutzrechtlichen Kontrolle und die Feststellung von Datenschutzverstößen zu machen. Das Geheimhaltungsinteresse der verantwortlichen Stelle muss zumindest dann zurückstehen, wenn sie rechtswidrig Daten verarbeitet.

2.3.1.4 Eingeschränkter Anwendungsbereich

Durch die Regelung zum räumlichen Anwendungsbereich des Gesetzes (§ 2 Abs. 4 ABDSG-E) wird eine Umgehung der nationalen Regelungen erleichtert.

Demnach fänden die Vorschriften nicht auf Anbieter Anwendung, die vom Ausland aus personenbezogene Daten im Inland verarbeiten.

2.3.1.5 Zweckerweiterung und Verstoß gegen Verhältnismäßigkeitsgrundsatz

Durch die teilweise unverhältnismäßigen und unbestimmten Tatbestände für die Verarbeitung personenbezogener Daten durch öffentliche Stellen im ABDSG-E (insb. § 4 ABDSG-E) sowie die vorgesehene Erweiterung der Möglichkeiten, Daten auch zu anderen Zwecken als jenen, zu denen sie erhoben worden sind, zu verarbeiten (vgl. § 6 ABDSG-E), wird der bisher mit dem BDSG vorgehaltene Datenschutzstandard mit dem ABDSG-E nicht mehr erreicht. Die Vorschrift zur Verarbeitung personenbezogener Daten durch öffentliche Stellen ist zu undifferenziert und wahrt nicht das Prinzip der Verhältnismäßigkeit. Insbesondere fehlt es an der Bestimmtheit und Normenklarheit. Die verfassungsrechtlich unabdingbare Klarstellung aus § 14 Abs. 1 BDSG, dass jeder öffentlichen Stelle die Datenverarbeitung nur dann erlaubt ist, wenn sie für eine Aufgabe erforderlich ist, für die die jeweilige öffentliche Stelle sachlich, funktional und örtlich zuständig ist, wurde nicht übernommen.

Die Vorschrift unterscheidet auch nicht mehr zwischen den einzelnen Verarbeitungsformen und ihren jeweiligen Zwecken. Ebenfalls zu weit geht die von § 4 ABDSG-E eröffnete Möglichkeit, dass beispielsweise ein Gesundheitsamt, allgemein und auch präventiv ohne konkreten Anlass, Daten zur Abwehr von Gefahren für die öffentliche Sicherheit oder aber, stellvertretend, zur Verfolgung von Straftaten oder Ordnungswidrigkeiten speichern könne.

Die Vorschriften bieten ein Einfallstor für die relativ undifferenzierte Speicherung einer Vielzahl von Daten auf Vorrat. Die Begriffe „Netz-, Daten- und Informationssicherheit“ in § 4 Abs. 2 Nr. 8 ABDSG-E sind nur wenig bestimmt und eine Befristung der Speicherdauer fehlt. Die bisherige Systematik des BDSG und der LDSG knüpft daran an, dass es für die konkrete Datenverarbeitung zur Aufgabenerfüllung weniger darauf ankommt, ob eine Aufgabe im öffentlichen Interesse liegt, als vielmehr darauf, ob der jeweiligen öffentlichen Stelle diese Aufgabe durch Gesetz zugewiesen ist. Diese Systematik sollte beibehalten werden. Die Zweckbindung ist seit jeher eines der zentralen Prinzipien des Datenschutzrechts. Sie dient der Transparenz und Vorhersehbarkeit der Verarbeitung personenbezogener Daten und stärkt damit die Autonomie der Betroffenen. Angesichts der Unsichtbarkeit und des Umfangs der Datenverarbeitung muss sich der Betroffene darauf verlassen können, dass seine personenbezogenen Daten grundsätzlich nur zu den Zwecken weiterverarbeitet werden, zu denen sie erhoben worden sind. Daher ist die Zweckbindung in Art. 8 Abs. 2 der Europäischen Grundrechtecharta als tragendes Prinzip des Datenschutzes verankert. Die Einhaltung der Zweckbindung ist ein Kernpunkt für ein funktionierendes Datenschutzrecht (vgl. Kernpunkte der DSK zu den Trilogverhandlungen).

Zweifelhaft ist bereits, ob der nationale Gesetzgeber überhaupt ermächtigt ist, die Ausnahmen von der Zweckbindung in § 6 ABDSG-E auch für den nicht-öffentlichen Bereich zu definieren. Jedenfalls sind Zweckänderungen bei nicht-öffentlichen Stellen in deutlich weniger Fällen zulässig als bei öffentlichen Stellen. Viele der in § 6 ABDSG-E genannten Zwecke können allenfalls für öffentliche Stellen innerhalb der jeweiligen Zuständigkeit gelten. Zudem führt die Vielzahl und weite Fassung der Ausnahmen zu einer völligen Aufweichung des Regel-Ausnahme-Prinzips. Die vorgesehenen Zweckerweiterungen bedürfen einer eingehenden Kontrolle hinsichtlich ihrer Zulässigkeit. Bei erlaubten Zweckänderungen ist das Prinzip der Verhältnismäßigkeit und der Ausnahmecharakter von Art. 6 Abs. 4 DS-GVO zu wahren.

2.3.1.6 Berufsgeheimnisträger

Mit der Regelung in § 36 ABDSG-E überschreitet der nationale Gesetzgeber seine Regelungskompetenz. Schon die Voraussetzungen aus Art. 23, 90 DS-GVO liegen nicht vor.

Der Regelungsbereich müsste danach differenzieren, ob es um die Datenschutzrechte derjenigen Person geht, die durch die Geheimhaltungspflicht geschützt wird, oder um Auskunfts- o. a. datenschutzrechtliche Begehren eines Dritten. Allenfalls im letzteren Fall wäre das Datenschutzrecht mit der Geheimhaltungspflicht abzuwägen.

Für die Beschränkung der Betroffenenrechte in § 36 S. 1 lit. a ABDSG-E besteht eine Öffnungsklausel nach Art. 23 Abs. 1 DS-GVO, die unzureichend ausgefüllt wird. Auch ist die Einhaltung der Voraussetzungen fraglich, da die Ausnahmen nach dem Wortlaut auch für die von den Geheimhaltungspflichten selbst geschützten Personen gelten.

Soweit es um die (Auskunfts-) Rechte von Dritten geht, wird nach gegenwärtigem Recht die Besonderheit der Schweigepflicht des Auskunftspflichtigen gemäß § 34 Abs. 7 in Verbindung mit § 33 Abs. 2 Satz 1 Nr. 3 BDSG berücksichtigt. Nach § 34 Abs. 7 BDSG besteht eine Pflicht zur Auskunftserteilung nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 BDSG nicht zu benachrichtigen ist. Gemäß § 33 Abs. 2 Nr. 3 BDSG entfällt die Pflicht zur Benachrichtigung, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen. Das ist zum Beispiel dann der Fall, wenn die begehrte Auskunft die anwaltliche Schweigepflicht des Auskunftspflichtigen gemäß § 43a BRAO berührt. Hier überwiegt das Recht des Rechtsanwalts auf ungestörte Berufsausübung das Interesse des Betroffenen auf Auskunftserteilung, weil der Betroffene die von ihm begehrten Informationen grundsätzlich auf direktem Weg durch Inanspruchnahme der Mandanten des Rechtsanwalts auf Auskunftserteilung erhalten kann.

Eine zusätzliche Beschränkung der Rechte der betroffenen Person gemäß Art. 23 Abs. 1 S. 2 DS-GVO in § 36 S. 1 lit. a ABDSG-E ist abzulehnen.

Die Regelung in § 36 S. 1 lit. b ABDSG-E ist ebenso wenig zulässig. Eine gesonderte Regelung für Beschränkungen der Aufsicht bei Berufsgeheimnisträgern ist weder notwendig noch verhältnismäßig, um das Recht auf Schutz der personenbezogenen Daten mit der Pflicht zur Geheimhaltung in Einklang zu bringen.

Eine Beschneidung der Aufsichtskompetenzen in diesem Bereich ist daher nicht indiziert. Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern werden häufig besonders schützenswerte Daten, wie z. B. Gesundheitsdaten, verarbeitet. Weder die Betroffenenrechte noch die unterstützende Kontrollkompetenz der Datenschutzbeauftragten dürfen hier beschnitten werden. Vielmehr ist eine wirksame datenschutzrechtliche Kontrolle, auch von Amts wegen, besonders vonnöten. Mit der Regelung in § 36 ABDSG-E wäre insbesondere in Fällen, in denen standesrechtliche Verstöße auf der Nichteinhaltung der Verschwiegenheitspflicht beruhen – bisher ein typischer datenschutzrechtlicher Prüffall bezogen auf Ärzte –, eine aufsichtsrechtliche Tätigkeit unmöglich, wenn sich der Berufsgeheimnisträger auch gegenüber der Aufsichtsbehörde auf die Verschwiegenheit berufen könnte.

Die Grundsätze, die das BVerfG in seinem Urteil vom 12.4.2005 (BVerfG, Beschluss vom 12.4.2005 – 2 BvR 1027/02 – s. Entwurfsbegründung) hervorgehoben hat und bei dem es um den Schutz der Verschwiegenheit im anwaltlichen Mandatsverhältnis gegenüber der Beschlagnahme durch staatliche Ermittlungsbehörden ging, sind nicht auf die Kontrolle durch unabhängige Aufsichtsbehörden übertragbar. Die Aufgabe der unabhängigen Aufsichtsbehörden besteht gerade in der Überprüfung der Geheimhaltung und der Einhaltung der datenschutzrechtlichen Anforderungen und nicht in der Verfolgung sonstiger Straftaten.

Wie bisher soll sich die Kontrollbefugnis der Datenschutzaufsichtsbehörden aufgrund der Regelungen in § 38 Abs. 3, 4 in Verbindung mit § 24 Abs. 6, 2 S. 1 Nr. 2 BDSG auch auf personenbezogene Daten beziehen, die einem Berufsgeheimnis unterliegen. Danach schränkt die anwaltliche Verschwiegenheitspflicht die Informationsrechte der Aufsichtsbehörden, die für die Datenschutzkontrolle zuständig sind, nicht ein („Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte“, Beschluss des Düsseldorfer Kreises vom 08./09.11.2007). Dementsprechend sind Rechtsanwälte nicht anders zu behandeln als jeder andere Berufszweig und als jede andere Gruppe von Freiberuflern (Thilo Weichert, Datenschutz auch bei Anwälten?, NJW 2009, 550 [552]).

Auch die Einschränkung der Rechte Dritter (s. o.) muss durch eine starke Kontrolle durch die Aufsichtsbehörden kompensiert werden. Auch diesem Zweck dient der gegenwärtige § 24 Abs. 2 S. 1 Nr. 2 BDSG. Zur Vermeidung von indirekter Ausforschung über die Aufsichtsbehörde könnte eine dem § 19 Abs. 6 BDSG entsprechende Regelung getroffen werden, wonach – wie es bisher etwa im Bereich strafrechtlicher Ermittlungsverfahren bewährte Praxis ist – die Aufsichtsbehörde dem Betroffenen nur mitteilt, ob datenschutzrechtliche Verstöße festgestellt wurden, nicht aber, ob und welche Daten die verantwortliche Stelle verarbeitet.

Gerade im Bereich der Tätigkeit von Berufsgeheimnisträgern dürfen weder die Betroffenenrechte noch die unterstützende Kontrollkompetenz der Datenschutzbeauftragten beschnitten werden.

Die Regelung des § 36 S. 2 ABDSG-E ist unbestimmt und zu weitreichend. Sie ist daher zu überarbeiten.

2.3.1.7 Datenverarbeitung zu wissenschaftlichen und statistischen Zwecken

Ein weiteres Beispiel für das sinkende Schutzniveau findet sich in § 34 Abs. 1 ABDSG-E. Dieser bleibt hinter den Anforderungen des § 14 Abs. 2 Nr. 9 und Abs. 5 Nr. 2 BDSG, insbesondere für besondere personenbezogene Daten, zurück. Bislang ist bei der Verarbeitung personenbezogener Daten zu Forschungszwecken in der Regel eine Einwilligung der betroffenen Personen erforderlich. Nur ausnahmsweise und unter engen gesetzlichen Voraussetzungen kann auf diese verzichtet werden.

Gemessen etwa an den differenzierten Regelungen des § 40 BDSG und in Art. 89 Abs. 1 S. 4 DS-GVO wird hier beispielsweise auf die gesetzliche Normierung eines "Stufenverhältnisses" (i. d. R. Verarbeitung anonymisierter Daten; nur wenn dies nicht geht: Verarbeitung pseudonymisierter Daten; nur wenn das nicht geht: Verarbeitung personenbezogener Daten; die beiden letzten Stufen allerdings nur unter der Voraussetzung weiterer konkret normierter Anforderungen) verzichtet. Wie die langjährige Erfahrung im Forschungsbereich zeigt, ist eine solche gesetzlich verankerte Differenzierung als Ausformung des Erforderlichkeitsgrundsatzes jedoch unverzichtbar.

§ 34 ABDSG-E unterscheidet nicht mehr zwischen sonstigen und besonderen personenbezogenen Daten und lässt bereits ein überwiegendes wissenschaftliches Interesse für die Verarbeitung auch sensibler Daten, wie genetischer, biometrischer und Gesundheitsdaten, ohne Einwilligung des Betroffenen, genügen. Zudem fehlen Vorgaben zu Sicherungs- und technisch-organisatorischen Maßnahmen.

Das Verhältnis der Regelungen zur Datenverarbeitung zu statistischen Zwecken zu den spezialgesetzlichen Statistikgesetzen ist unklar und enthält in der vorliegenden Form inkonsistente Doppelregelungen.

2.3.2 Stellung der unabhängigen Datenschutzaufsichtsbehörden der Länder

Die Einführung eines Klagerechts für die unabhängigen Datenschutzaufsichtsbehörden wird begrüßt, bedarf aber einer Erweiterung. Die Ausgestaltung der Regelungen zur Vertretung der Aufsichtsbehörden im Europäischen Datenschutzausschuss und zur Zusammenarbeit ist zwischen der BfDI und den unabhängigen Aufsichtsbehörden der Länder umstritten, bedarf aber in jedem Fall der Überarbeitung.

2.3.2.1 Klagerecht

Die Schaffung eines Klagerechts, wie in § 28 ABDSG vorgesehen, wird begrüßt. Vor dem Hintergrund der Möglichkeiten in Art. 58 Abs. 5 DS-GVO und Art. 47 Abs. 5 JI-RL ist der Anwendungsbereich jedoch zu eng. Durch die Verwendung des allgemeinen Begriffes „Verstöße“ in den Art. 58 Abs. 5 DS-GVO und Art. 47 Abs. 5 JI-RL kommt der Wunsch des europäischen Verordnungs- bzw. Richtliniengebers zum Ausdruck, für möglichst viele Maßnahmen den Rechtsweg zu eröffnen. Dies betrifft nicht nur Angemessenheitsentscheidungen nach Artikel 45 DS-GVO, sondern auch andere Rechtsakte der Kommission, wie beispielsweise Standardvertragsklauseln und andere abstrakt-generelle Regelungen, unabhängig davon, ob diese von der Europäischen Kommission oder vom nationalen Gesetzgeber erlassen werden. Insbesondere muss eine abstrakte Klärung unabhängig vom Vorliegen einer Beschwerde von Betroffenen möglich sein. Eine Erweiterung des Klagerechts in diesem Sinne würde es dem EuGH ermöglichen, die unionsweit einheitliche Rechtsanwendung zu kontrollieren und somit zur Harmonisierung des Datenschutzrechts beizutragen.

2.3.2.2 Vertretung im Europäischen Datenschutzausschuss

Wie die Vertretung im Europäischen Datenschutzausschuss zu erfolgen hat, ist zwischen der BfDI und den unabhängigen Datenschutzaufsichtsbehörden der Länder umstritten.

Die Formulierung in § 29 ABDSG-E entspreche aus Sicht der Aufsichtsbehörden der Länder nicht der föderalen Kompetenzordnung des Grundgesetzes. § 29 Abs. 2 ABDSG-E sei bereits missverständlich formuliert. Nach der Gesetzesbegründung könne der Stellvertreter „gemäß Absatz 2 von dem gemeinsamen Vertreter verlangen, die Verhandlungsführung und das Stimmrecht übertragen zu erhalten, soweit die Angelegenheit in die sachliche

Alleinzuständigkeit der Länderaufsichtsbehörden fällt". Die Gesetzesbegründung knüpfe demnach an die Vollzugstätigkeit an. Der Gesetzesvollzug ist im Datenschutz überwiegend den Ländern übertragen. Der Gesetzeswortlaut beziehe sich hingegen eher auf die ausschließliche Gesetzgebungskompetenz der Länder. Wegen der vielfach konkurrierenden Gesetzgebungskompetenz könne damit das Stimmrecht bei der BfDI verbleiben, obgleich die Vollzugszuständigkeit bei den Ländern liege.

Für die Anknüpfung an die Vollzugskompetenz spreche zunächst, dass die Vertretung im Ausschuss Verwaltungshandeln betreffe und die Verwaltung nach den Vorgaben des Grundgesetzes grundsätzlich Angelegenheit der Länder sei. Die überwiegende Mehrheit der im Ausschuss zu behandelnden Angelegenheiten dürfte die Datenschutzaufsicht gegenüber nicht-öffentlichen Stellen betreffen. Diese sei und bleibe im Wesentlichen den Aufsichtsbehörden der Länder vorbehalten. Diese seien die für die nicht-öffentlichen Stellen in Art. 51 Absatz 1 DS-GVO genannten unabhängigen Aufsichtsbehörden und unterlägen selbst der Verpflichtung nach Art. 51 Abs. 2 DS-GVO, einen Beitrag zur einheitlichen Anwendung der DS-GVO zu leisten („Jede Aufsichtsbehörde"). Damit liege es nach der bundesstaatlichen Aufgabenverteilung mehr als nahe, in allen Angelegenheiten, die diese Zuständigkeit der Länder betreffen, entsprechend der Gesetzesbegründung dem Vertreter der Länder auf dessen Verlangen die Verhandlungsführung und das Stimmrecht zu übertragen. Nur so könnten ein Leerlaufen des Länderstimmrechts und ein Widerspruch mit der Vollzugspraxis der Länder verhindert werden.

Auch das Konzept, wonach der/die BfDI dauerhaft als Vertreter/in gesetzt ist, während die Stellvertretung stets der Ländervertretung zufällt, erscheine vor dem Hintergrund der aufsichtsbehördlichen Landeskompetenzen nicht plausibel.

Die Unabhängigkeit der Datenschutzbeauftragten lege zudem eine Wahl des Ländervertreters durch die Aufsichtsbehörden der Länder selbst nahe.

Demgegenüber begrüßt die BfDI die in § 29 Abs. 1 ABDSG-E festgelegte Zuweisung der Aufgabe des gemeinsamen Vertreters nach Art. 68 Abs. 4 DS-GVO an die BfDI und unterstützt die in der Begründung dafür genannten Gründe. Die Stellung des Landesvertreters als Stellvertreter i. S. v. Art. 68 Abs. 3 DS-GVO begegne aus ihrer Sicht ebenfalls keinen Einwänden.

Die Zuständigkeitsübertragung auf den Landesvertreter (§ 29 Abs. 2 ABDSG-E) regele nach ihrer Auffassung drei Fallvarianten, in denen die BfDI dem Landesvertreter die Verhandlungsführung und das Stimmrecht im EDSA übertragen müsse. Dies sei neben der ausschließlichen Gesetzgebungszuständigkeit der Länder und der Einrichtung von Landesbehörden auch „das Verfahren von Landesbehörden". Die BfDI legt der Formulierung des Gesetzestextes das Verständnis zugrunde, dass mit „Verfahren von Landesbehörden" nicht dasjenige vor den Aufsichtsbehörden i. S. v. § 27 ABDSG-E gemeint sei, sondern allgemein das Verfahren von (anderen) Landesbehörden, d. h. der öffentliche Bereich der Länder. Um dies deutlich zu machen und jeden Zweifel auszuschließen, solle die Begründung eindeutig und präzise klarstellen, dass sich „Verfahren von Landesbehörden" ausschließlich auf solche außerhalb der Datenschutzaufsichtsbehörden beziehe und deren Verfahren (d. h. der nicht-öffentliche Bereich) hier nicht gemeint seien. Die BfDI hält die Übertragung der Aufgabe des gemeinsamen Vertreters auf ihre Behörde auch für sachgerecht, da sie die notwendige Kontinuität sichern könne, eine langjährige Erfahrung im Bereich des europäischen Datenschutzes habe und am ehesten über die erforderlichen Ressourcen verfüge.

Einigkeit besteht darüber, dass eine Klarstellung im Gesetz wünschenswert ist, wonach der gemeinsame Vertreter und sein Stellvertreter sich bei Abwesenheit gegenseitig vertreten können, was eine Vertretung durch Mitarbeiter jedoch nicht ausschließt.

2.3.2.3 Einrichtung einer zentralen Anlaufstelle

Hinsichtlich der Einrichtung der zentralen Anlaufstelle bei der BfDI (vgl. § 29 Abs. 1 S. 1 ABDSG-E) ist eine Klarstellung erforderlich, dass die zentrale Anlaufstelle nicht selbst Aufgaben wahrnimmt, für die die anderen Aufsichtsbehörden (namentlich die Aufsichtsbehörden der Länder nach § 27 ABDSG-E) zuständig sind, sondern dass der zentralen Anlaufstelle allein eine unterstützende Funktion zukommt. Ausweislich des Wortlauts des Erwägungsgrunds 119 DS-GVO soll die zentrale Anlaufstelle die Beteiligung der anderen in einem Mitgliedstaat existierenden Datenschutzaufsichtsbehörden sicherstellen, nicht jedoch selbst die Beteiligung wahrnehmen oder ersetzen. Aus Gründen der Rechtsklarheit ist dies im Gesetzestext selbst zu verdeutlichen. Es muss sichergestellt sein, dass auch die Aufsichtsbehörden der Länder nach § 27 ABDSG-E in gleicher Weise effektiv an der Willensbildung im Europäischen Datenschutzausschuss teilnehmen können, wie bislang im Rahmen der Artikel 29-Gruppe und deren Arbeitsgruppen. Auch wenn die zentrale Anlaufstelle von der BfDI bereitgestellt wird, ist eine eindeutige Trennung im Hinblick auf Organisation und Berichtspflichten zwischen der zentralen Anlaufstelle und dem übrigen Personal der BfDI unerlässlich. Als Modell könnte insoweit die Stellung des Sekretariats des

Europäischen Datenschutzausschusses (Art. 75 DS-GVO) dienen, das vom Europäischen Datenschutzbeauftragten bereitgestellt wird. Ähnlich wie das Sekretariat nimmt auch die zentrale Anlaufstelle nur unterstützende Aufgaben wahr. Leitlinie für die zentrale Anlaufstelle muss es sein, ein Gleichgewicht in Hinblick auf die effektive Mitwirkung aller deutschen Datenschutzaufsichtsbehörden an der Willensbildung im Europäischen Datenschutzausschuss auch an dieser Stelle zu gewährleisten.

2.3.2.4 Zusammenarbeit

Hinsichtlich der in § 30 ABDSG-E getroffenen Regelungen über die Zusammenarbeit wird auf den Beschluss „Vorschläge zu ersten Strukturfolgerungen aus der DS-GVO“ nebst Ablage der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 6./7. April 2016 in Schwerin verwiesen.

Danach sind Zuständigkeitsregelungen sowie die Beteiligung in den Verfahren der Zusammenarbeit und der Kohärenz, soweit sie Außenwirkung entfalten, durch Gesetz zu treffen. Dieses sollte sich darauf beschränken, die Aufsichtsbehörden zu verpflichten, in den erforderlichen Fällen eine Abstimmung mit dem Ziel der einheitlichen Votierung vorzunehmen. Die Einzelheiten sollten die unabhängigen Aufsichtsbehörden autonom regeln.

Eine weitergehende Stellungnahme hierzu ist beabsichtigt.

2.3.2.5 Ergänzung zur örtlichen Zuständigkeit

Wünschenswert ist schließlich eine Klärung der örtlichen Zuständigkeit im nicht-öffentlichen Bereich, soweit kein grenzüberschreitender Bezug vorliegt. Bei der örtlichen Zuständigkeit der Aufsichtsbehörden weichen derzeit Praxis und Recht gelegentlich voneinander ab. Die Verwaltungsverfahrensgesetze der Länder legen i. d. R. eine Anknüpfung an die Betriebsstätte nahe, während verbreitete Praxis der Aufsichtsbehörden eine Orientierung am Sitz der verantwortlichen Stelle ist. Beides ist inkompatibel mit dem Prinzip der DS-GVO, an der Hauptniederlassung anzuknüpfen.

2.3.3 Beschäftigtendatenschutz

Es wird begrüßt, dass das ABDSG-E von der Regelungsbefugnis des Art. 88 DS-GVO zumindest durch Übernahme der bisherigen Regelungen des BDSG Gebrauch macht, insbesondere vor dem Hintergrund, dass sich die Ausgestaltung der Beschäftigungsverhältnisse in Deutschland deutlich von der in anderen Mitgliedstaaten unterscheidet. Das Arbeitsrecht im weitesten Sinne ist ein stark national geprägter Rechtsbereich, weshalb bewährte Mechanismen und Grundsätze trotz europäischer Harmonisierung soweit möglich beibehalten werden sollten. Die Forderung eines bereichsspezifischen Beschäftigtendatenschutzes bleibt bestehen. Deshalb kann die Übernahme der bisherigen Regelung auch in Hinblick auf die zu beachtenden Anforderungen des Art. 88 Abs. 2 DS-GVO nur als Merkposten für die Schaffung eines überzeugenden nationalen Beschäftigtendatenschutzes gelten.

2.3.4 Betriebliche Datenschutzbeauftragte

Zuzustimmen ist auch den Regelungen in den §§ 14 f. ABDSG-E zum betrieblichen Datenschutzbeauftragten. Jedoch sollte das Merkmal der Zuverlässigkeit (keine Interessenkollision, persönliche Integrität) ergänzt und sichergestellt werden, dass die bisherigen flankierenden Regelungen, wie z.B. zum Abberufungsschutz (vgl. § 4f Abs. 3 S. 4 BDSG), vollumfänglich erhalten bleiben. Die Pflicht zur Meldung der/des benannten Datenschutzbeauftragen sollte auch weiterhin gegenüber der zuständigen Aufsichtsbehörde bestehen (§ 14 Abs. 4 S. 1 und S. 2 ABDSG-E).

2.3.5 Akkreditierung

Die Doppelzuständigkeit für die Akkreditierung in § 16 ABDSG-E ist hinsichtlich einer gleichmäßigen Akkreditierung kontraproduktiv. Die Akkreditierung sollte vorzugsweise denjenigen Stellen überlassen werden, welche über große Expertise und Kenntnisse im Bereich des Datenschutzes verfügen. Dies sind die Fachaufsichtsbehörden für den Datenschutz, welche einheitliche Akkreditierungskriterienkataloge erstellen und im Rahmen eines einheitlichen Akkreditierungsverfahrens anwenden.

2.3.6 Videoüberwachung

Die Verarbeitung durch Videoüberwachung erhobener personenbezogener Daten durch öffentliche Stellen des Bundes ist nur unzureichend geregelt. Es fehlen Regelungen zur Erhebung der Daten, was insbesondere auch dann relevant wird, wenn eine Beobachtung ohne Speicherung erfolgt, sowie zur Weiterverarbeitung gespeicherter Daten zu anderen Zwecken. Die entsprechenden Regelungen aus dem BDSG werden nicht vollständig übernommen. Notwendig sind insbesondere die Normierung einer engen Zweckbestimmung sowie die ausdrückliche Verankerung des Erforderlichkeits- und Verhältnismäßigkeitsprinzips. Zudem sind die Regelungen zur Einschränkung der Informationspflichten zu weitgehend und bleiben hinter dem Datenschutzniveau der DS-GVO zurück.

So regelt § 7 Abs. 3 S. 1 ABDSG-E, dass die Informationspflicht bei öffentlicher und nicht-öffentlicher Videoüberwachung entfällt. § 7 Abs. 3 S. 2 ABDSG-E bestimmt, dass in diesem Fall der Umstand der Beobachtung und der Verantwortliche durch geeignete Maßnahmen erkennbar gemacht werden solle.. Insoweit ist § 7 Abs. 3 S. 2 ABDSG-E fast wortgleich mit § 6b Abs. 2 BDSG. Die Erkennbarmachung der Videoüberwachung erfolgt in der Praxis z. B. durch Anbringen eines Piktogramms gemäß DIN 33450 in Verbindung mit der Anschrift der verantwortlichen Stelle.

Die (umfassendere) Informationspflicht gemäß Artikel 13 DS-GVO wird nunmehr bezüglich der Videoüberwachung durch öffentliche wie auch durch nicht-öffentliche Stellen eingeschränkt. Das Recht auf Information aus Art. 13 Abs. 3 und 4 DS-GVO soll gemäß § 7 Abs. 2 ABDSG-E entfallen, soweit die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde. Diese Beschränkung der Informationspflicht diene - so der Entwurf – dem Schutz der Rechte und Freiheiten anderer Personen (Art. 23 Abs. 2 lit. c und Abs. 1 lit. i DS-GVO).

Damit verkennt der Gesetzentwurf die Intention des Art. 23 DS-GVO.

Nach der Gesetzessystematik der DS-GVO können Pflichten und Rechte der DS-GVO gemäß Art. 23 beschränkt werden. Dazu gehören auch die Informationspflichten gemäß Art. 13 DS-GVO. Diese Beschränkungen dürfen jedoch nicht den Wesensgehalt der Grundrechte und Grundfreiheiten tangieren und müssen eine in der demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme darstellen. Diese Maßnahmen sollen nach Art. 23 Abs. 1 lit. a-h DS-GVO öffentliche Belange der Sicherheit, Justiz und des Ordnungsrechts sicherstellen. Art. 23 Abs. 1 lit. i und j DS-GVO betreffen den privaten Bereich. Artikel 23 Abs. 1 lit. I DS-GVO soll den Schutz der betroffenen Personen oder der Rechte und Freiheiten anderer Personen sicherstellen.

Die Beschränkung der Informationspflichten durch § 7 Abs. 2 ABDSG-E wegen unverhältnismäßigen Aufwandes der Informationserteilung schafft hingegen nur Erleichterungen für den Verantwortlichen der Videoüberwachung. Dies widerspricht aber gerade Sinn und Zweck des Art. 23 DS-GVO. Hiernach soll der Schutz der betroffenen Personen und der Rechte und Freiheiten anderer Personen durch die Beschränkung sichergestellt werden. Im Entwurf wird zudem nur geregelt, dass der Verantwortliche Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person zu ergreifen hat. Gemäß Art. 23 Abs. 2 DS-GVO müssen dafür aber ggf. spezifische Vorschriften in Bezug auf den Umfang der vorgenommenen Beschränkung geschaffen werden. Die Überleitung des Schutzzwecks der Maßnahme auf die verantwortliche Person ist vor dem Hintergrund des Art. 23 DS-GVO nicht ausreichend, weil eine konkretisierende Regelung wie in Art. 14 Abs. 5 lit. b DS-GVO fehlt.

Nicht mehr vorgesehen ist eine Regelung wie in § 6b Abs. 4 BDSG über die Informationspflicht für den Fall, dass die Daten aus einer Videoüberwachung einer bestimmten Person zugeordnet werden. Hierbei handelt es sich um eine Identitätsverknüpfung, von der die betroffene Person nicht mit einem bloßen Hinweis auf die Videoüberwachung Kenntnis erlangen kann. Der Schutz der Rechte der betroffenen Personen wird mit dieser Regelung keinesfalls sichergestellt.

Schließlich sollte, soweit dies nach den Öffnungsklauseln möglich ist, eine Regelung bzw. Klarstellung in Bezug auf ein Verbot der heimlichen Videoüberwachung erfolgen.

2.3.7 Auskunfteien

Die Übernahme der Vorschrift des § 28a BDSG entspricht dem ganz überwiegenden Wunsch der Aufsichtsbehörden, auch wenn die europarechtliche Anknüpfung diskutiert wird. Sie wird daher grundsätzlich begrüßt.

Die Löschfristen für Auskunfteien in § 35 Abs. 2 S. 2 Nr. 4 BDSG sowie die Regelung zur Auskunftserteilung nach § 34 Abs. 8 BDSG sollten ebenfalls übernommen werden.

2.3.8 Scoring

Zuzustimmen ist auch der Übernahme von § 28b BDSG. Die entsprechende Regelung bedarf aber einer deutlichen Verbesserung.

2.4 Regelungen zur Durchsetzbarkeit der DS-GVO

Nach Art. 58 Abs. 5 DS-GVO muss jeder Mitgliedstaat durch Rechtsvorschriften dafür sorgen, dass die jeweiligen unabhängigen Aufsichtsbehörden die DS-GVO in den Mitgliedstaaten auch durchsetzen können. Dieser Aufforderung sollte insbesondere im Bereich der Verwaltungs- und Bußgeldvorschriften Rechnung getragen werden.

2.4.1 Verwaltungsverfahren

Die DS-GVO muss gegenüber öffentlichen und nicht-öffentlichen Stellen gleichermaßen durchsetzbar sein. Insoweit unterscheidet die DS-GVO nicht. Es fehlt daher zunächst eine Regelung zur Vollstreckung von Verwaltungsakten gegenüber Behörden und sonstigen öffentlichen Stellen. § 17 VwVG schließt, ebenso wie die meisten Verwaltungsvollstreckungsregelungen der Landesgesetze, unter Berücksichtigung des koordinationsrechtlich geprägten Verhältnisses zwischen Hoheitsträgern den Vollzug gegen Behörden und juristische Personen des öffentlichen Rechts aus, soweit nicht etwas anderes bestimmt ist. Hier besteht Handlungsbedarf. Einerseits bedarf es zumindest einer Klarstellung, ob entsprechend der Regelung in § 42 Abs. 3 S. 2 ABDSG-E die Vollstreckung gegen öffentliche Stellen, die mit anderen Verarbeitern im Wettbewerb stehen, möglich ist. Darüber hinaus ist es mit den Grundsätzen der DS-GVO kaum vereinbar, wenn den Aufsichtsbehörden gegenüber Behörden und sonstigen öffentlichen Stellen i. S. d. § 2 Abs. 1 ABDSG-E kein Mittel zur Seite gestellt wird, datenschutzrechtliche Verstöße auch tatsächlich abzustellen. Jedenfalls für gerichtlich festgestellte Verstöße verlangt Art. 58 Abs. 5 DS-GVO, dass der nationale Gesetzgeber die Aufsichtsbehörde in die Lage versetzt, die Bestimmungen dieser Verordnung durchzusetzen und nicht lediglich mögliche Verstöße feststellen zu lassen. Bei dieser bloßen Beanstandung durch die Aufsichtsbehörden verbliebe es aber faktisch, wenn im ABDSG-E keine Regelung aufgenommen wird, die die Vollstreckung gegen Behörden und sonstige öffentliche Stellen zulässt.

Fragwürdig erscheint auch der Ausschluss der Anordnung der sofortigen Vollziehung gegenüber öffentlichen Stellen mit Ausnahme der Wettbewerbsunternehmen. Auch im öffentlichen Bereich wird es Fälle geben, in denen die Anordnung der sofortigen Vollziehung notwendig ist, um die Rechte der Betroffenen zu wahren. Angesichts der Dauer verwaltungsgerichtlicher Streitigkeiten ist diese Möglichkeit in dringenden Eilfällen unverzichtbar. Ordnet die BfDI bspw. die Beseitigung einer Sicherheitslücke in einem IT-System einer Behörde an, darf eine Klage der Behörde nicht dazu führen, dass wegen der aufschiebenden Wirkung dieser Zustand auf unbestimmte Dauer anhält. Ein Rechtsschutzdefizit der öffentlichen Stellen ist ebenfalls nicht ersichtlich. Wie jeder andere Adressat der aufsichtsbehördlichen Maßnahmen hätten sie die Möglichkeit, gemäß § 80 Abs. 5 VwGO die Wiederherstellung der aufschiebenden Wirkung zu beantragen. Ob der in der Begründung als Alternative angesprochene Antrag auf einstweilige Anordnung statthaft wäre, ist zu bezweifeln. Dieser ist ein Rechtsschutzinstrument gegen (drohende) Maßnahmen von Behörden, ermöglicht es aber den Behörden nicht, ihrerseits Aufsichtsbefugnisse im Eilfall mit Hilfe des Gerichts durchzusetzen.

2.4.2 Ordnungswidrigkeitenverfahren

Die Frage, ob Bußgelder gegen Behörden und sonstige öffentliche Stellen verhängt werden können, sollte im Ermessen der Aufsichtsbehörden liegen. Des Weiteren müssen Bußgeldtatbestände und Verweise auf Vorschriften des OWiG ergänzt werden. Zuzustimmen ist den Regelungen zur Zuständigkeit der Landgerichte und der Verfahrensbeteiligung der Aufsichtsbehörden im gerichtlichen Verfahren.

2.4.2.1 Bußgelder gegen öffentliche Stellen

Vor dem Hintergrund der notwendigen Durchsetzbarkeit der DS-GVO ist die Vorschrift in § 42 Abs. 3 ABDSG-E, wonach gegen Behörden und sonstige öffentliche Stellen mit Ausnahme der Wettbewerbsunternehmen keine Bußgelder verhängt werden sollen, zu hinterfragen. Der im Bereich der DS-GVO nicht anwendbare § 30 OWiG schließt Bußgelder gegen juristische Personen des öffentlichen Rechts nicht aus, allerdings wird hier immer wieder kritisch angemerkt, dass Bußgelder gegen juristische Personen des öffentlichen Rechts ihre sanktionierende Wirkung verfehlen und Gelder im öffentlichen Haushalt lediglich die Titel wechseln. Für Verstöße gegen die DS-GVO kommt hinzu, dass Bußgelder, anders als Zwangsmittel, die Durchsetzung der DS-GVO nicht unmittelbar erzwingen können.

Allerdings sollte die Entscheidung in das pflichtgemäße Ermessen der unabhängigen Datenschutzaufsichtsbehörden gestellt werden.

2.4.2.2 Weitere Bußgeldtatbestände

Soweit man für § 42 Abs. 1 ABDSG-E eine Regelungskompetenz des nationalen Gesetzgebers bejaht, sollten die auf Mitarbeiter erweiterten Bußgeldtatbestände ausformuliert und nicht lediglich auf Art. 83 DS-GVO verwiesen werden. Geht man davon aus, dass die Tatbestände, auf die Art. 83 DS-GVO verweist, nur für Verantwortliche oder Auftragverarbeiter gelten, besteht zwar eine Regelungskompetenz, allerdings muss dann ein neuer Tatbestand formuliert werden, der nicht auf Verantwortliche beschränkt ist. In der derzeitigen Fassung genügt die Vorschrift nicht dem Bestimmtheitsgebot. Geht man indes davon aus, dass Art. 83 DS-GVO nebst Verweisen auch für Mitarbeiter gilt, besteht keine Regelungskompetenz des nationalen Gesetzgebers.

Zudem wird die Bußgeldgrenze ohne nähere Begründung in Anlehnung an die bislang geltende Regelung im BDSG auf 300.000 Euro beschränkt. Wenn man davon ausgehen sollte, dass Mitarbeiter von verantwortlichen Stellen nicht vom Regelungsgehalt des Art. 83 DS-GVO erfasst werden und den Mitgliedstaaten insoweit ein eigenes Regelungsrecht zukommt, sollten sich entsprechende Bußgeldbestimmungen jedenfalls an den in der DS-GVO genannten Bußgeldgrenzen orientieren. Da nach Art. 83 Abs. 1 DS-GVO Geldbußen verhältnismäßig sein müssen, besteht auch keine Gefahr der übermäßigen Belastung von Mitarbeitern durch die Festlegung zu hoher Geldbußen für einen von ihnen zu verantwortenden Verstoß.

Darüber hinaus sollten weitere Bußgeldtatbestände ergänzt werden.

Sofern der Gesetzgeber davon ausgeht, dass die DS-GVO keinen Bußgeldtatbestand wegen nicht erteilter Auskunft gegenüber der Aufsichtsbehörde enthält, wäre ein solcher entsprechend § 43 I Nr. 10 BDSG zu schaffen. Ohne einen solchen Bußgeldtatbestand ist eine wirksame Aufsichtstätigkeit nicht denkbar. Verstöße gegen die in § 33 ABDSG-E aufgenommene Regelung für die Datenverarbeitung im Beschäftigtenkontext sind ebenfalls nicht explizit bußgeldbewährt. Darüber hinaus fehlt es in § 42 Abs. 2 ABDSG-E an einem Bußgeldrahmen.

2.4.2.3 Zuständigkeit der Landgerichte

Zu befürworten ist die Regelung zur Zuständigkeit des Landgerichts für die Prüfung von Bußgeldbescheiden über 5.000 Euro. Hierfür spricht zum einen die gravierende Erhöhung des Bußgeldrahmens von 300.000 Euro nach dem derzeit geltenden BDSG auf bis zu 20 Millionen Euro bzw. bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres im Falle eines Unternehmens gemäß Art. 83 Abs. 4 bis 6 DS-GVO. Zum anderen legt dies auch die Übernahme des kartellrechtlichen funktionalen Unternehmensbegriffs in der DS-GVO nahe, da die Regelungen zur gerichtlichen Zuständigkeit in Kartellverfahren sogar das Oberlandesgericht als Eingangsinstanz bestimmen (vgl. § 83 Abs. 1 Gesetz gegen Wettbewerbsbeschränkungen – GWB).

2.4.2.4 Beteiligung der Aufsichtsbehörden im gerichtlichen Verfahren

Ebenfalls zu befürworten ist, dass gemäß § 50 Abs. 1 S. 4-8 ABDSG-E zukünftig die Aufsichtsbehörden anstelle der Staatsanwaltschaft direkte Beteiligte in Gerichtsverfahren über datenschutzrechtliche Bußgeldbescheide werden sollen. Zum einen wird hierbei der Expertise der Aufsichtsbehörden in Datenschutzangelegenheiten Rechnung getragen und somit die Qualität der gerichtlichen Auseinandersetzung bedeutend gestärkt. Zum anderen wird dadurch die in Art. 52 Abs. 1 DS-GVO normierte „völlige“ Unabhängigkeit der Aufsichtsbehörden gewährleistet.

2.4.2.5 Anwendbarkeit OWiG

Es wird begrüßt, dass die Regelungen des OWiG nicht pauschal für anwendbar erklärt werden und insbesondere § 130 OWiG keine Anwendung findet. Dem europarechtlich geltenden funktionalen Unternehmensbegriff (vgl. Art. 101, 102 AEUV) wird so hinreichend Rechnung getragen.

Dennoch fehlen Verweise auf Bestimmungen des OWiG. So sollte § 3 OWiG (Bestimmtheitsgebot) für anwendbar erklärt werden. Ferner bestehen keine Bedenken gegen die Anwendung von § 29 OWiG. Die §§ 40 - 44 OWiG regeln die Zuständigkeit der Staatsanwaltschaft für Strafsachen, die Abgabe an die Staatsanwaltschaft sowie ggf. die Rückgabe an die Verwaltungsbehörde. Sollte die Staatsanwaltschaft eine Strafsache einstellen, verbliebe für die Aufsichtsbehörde weiterhin die Möglichkeit, ein Bußgeld festzusetzen (§ 41 Abs. 2, § 43 Abs. 1 OWiG). Die Anwendung von § 40 OWiG müsste daher mit der Maßgabe erfolgen, dass eine Einstellung hinsichtlich der die Straftat „begleitenden“ Ordnungswidrigkeit nur im Einvernehmen mit der Aufsichtsbehörde möglich ist.

Kritisch gesehen wird auch die Regelung in § 60 ABDSG-E. Da dieser aber auf den Anwendungsbereich der JI-Richtlinie beschränkt ist, erfolgen Ausführungen hierzu wie angekündigt gesondert.

2.5 Gestaltung des Medienprivilegs

Art. 85 Abs. 2 DS-GVO enthält einen Auftrag an die Mitgliedstaaten, Ausnahmen von bestimmten Kapiteln der DS-GVO zu regeln, soweit dies erforderlich ist, um bei der Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen oder literarischen Zwecken das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang zu bringen.

Der Gesetzgeber sollte das so genannte „Medienprivileg“ in klaren Regelungen gestalten, um mit praktikablen Kriterien Klarheit über die künftige Reichweite zu schaffen und um hierbei auch die bereits bestehende Rechtsunsicherheit bezüglich der Privilegierung von teilweise redaktionell bearbeiteter Meinungsverbreitung über das Internet zu beseitigen.

Sachwortverzeichnis zum 45. Tätigkeitsbericht