Vierundvierzigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2015

gemäß § 30 des Hessischen Datenschutzgesetzes

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

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

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

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 44. Tätigkeitsbericht

Abb.	Abbildung
Abs.	Absatz
AFBG	Gesetz zur Förderung der beruflichen Aufstiegsfortbildung
AG	Aktiengesellschaft
AKB	Allgemeine Bedingungen für die Kraftfahrzeugversicherung
AO	Abgabenordnung
App	Application (Anwendungssoftware für mobile Betriebssysteme)
Art.	Artikel
AStV	Ausschuss der ständigen Vertreter
Aufl.	Auflage
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BCR	Binding Corporate Rules (verbindliche Unternehmensregeln)
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BSI	Bundesamt für Sicherheit in der Informationstechnik
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	circa
cm	Zentimeter
CoC	Code of Conduct (Verhaltenskodex)
CTI	Computer Telefonie Integration
d. J.	dieses Jahres
DAPIX	Arbeitsgruppe „Informationsaustausch und Datenschutz“
DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
e. V.	eingetragener Verein
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDV	Elektronische Datenverarbeitung
EES	Einreise-/Ausreisesystem
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
FATCA	Foreign Account Tax Compliance Act
FAZ	Frankfurter Allgemeine Zeitung
FTC	Federal Trade Commission (Amerikanische Handelkommission)
GewO	Gewerbeordnung
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz)
HbbTV	Hybrid Broadcast Broadband TV
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HeFIS	Hessisches Forschungsinformationssystem
HGB	Handelsgesetzbuch
HMDIS	Hessisches Ministerium des Innern und für Sport

HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
IP	Internet Protokoll
IQB-Ländervergleich	Überprüfung von Bildungsstandards
IT	Informationstechnik
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, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssystem
KOM	Europäische Kommission
KVH	Kassenärztliche Vereinigung Hessen
LÄK	Landesärztekammer
LTSB	Long Time Service Branch
MDM	Mobile Device Management
Nadis	Nachrichtendienstliches Informationssystem
NEPS	National Educational Panel Study
NFC	Near Field Communication (Nahfeldkommunikation)
NRW	Nordrhein-Westfalen
OH KIS	Orientierungshilfe für Krankenhausinformationssysteme
PISA	Internationale Schulleistungsuntersuchungen
Rdnr.	Randnummer
RGBl.	Reichsgesetzblatt
RTP	Programm für registrierte Vielreisende
S.	Seite *oder* Satz
s.	siehe
SEPA	Single Euro Payments Area
SGB	Sozialgesetzbuch
SIS II	Schengener Informationssystem der zweiten Generation
SMS	Short Message Service
sog.	sogenannte/r/s
StAnz.	Staatsanzeiger für das Land Hessen
StVG	Straßenverkehrsgesetz
TK	Telekommunikation
TLS/SSL	Transport Layer Security/Secure Sockets Layer
TMG	Telemediengesetz
TV	Fernsehgerät (Televisison)
u. a.	unter anderem
u. Ä.	und Ähnliches
UM	Unified Messaging
UmsV	Umsetzungsverordnung

US	United States
USA	Vereinigte Staaten von Amerika
usw.	und so weiter
VAG	Versicherungsaufsichtsgesetz
vgl.	vergleiche
WEG	Wohnungseigentumsgesetz
z. B.	zum Beispiel
Ziff.	Ziffer

Register der Rechtsvorschriften

AFBG	Gesetz zur Förderung der beruflichen Aufstiegsfortbildung (Aufstiegsfortbildungsförderungsgesetz) i. d. F. vom 08.10.2012 (BGBl. I S. 2126),
AO	Abgabenordnung i. d. F. vom 01.10.2002 (BGBl. I S. 3866,. 2003 I S. 61), zuletzt geändert durch Gesetz vom 03.12.2015 (BGBl. I S. 2178)
Artikel 29-Datenschutzgruppe WP 187	Stellungnahme 15/2011 zur Definition von Einwilligung vom 13.07.2011 (01197/11/DE) http://ec.europa.eu/justice/policies/privacy/index_de.htm
BAföG	Gesetz über individuelle Förderung der Ausbildung i. d. F. vom 07.12.2010 (BGBl. I S. 1952), zuletzt geändert durch Gesetz vom 27.07.2015 (BGBl. I S. 1386)
BDSG	Bundesdatenschutzgesetz i. d. F. vom 14.01.2003 (BGBl. S. 66), zuletzt geändert durch Gesetz vom 25.02.2015 (BGBl. I S. 162)
Beschluss 2007/533/JI des Rates der EU über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation(SIS II)	vom 12.06.2007 (ABl. L 205/63)
Beschluss der EU-Kommission 2010/87/EU über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates	vom 05.02.2010, Az. K(2010) 593 (ABl. L 39/5)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 S. 738), zuletzt geändert durch Gesetz vom 21.04.2015 (BGBl. I S. 610)
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz) i. d. F. vom 21.09.1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 21.01.2015 (BGBl. I S. 10)
Datenschutz im öffentlichen Bereich; hier: Durchführung der §§ 6 (Verfahrensverzeichnis) und 15 (Gemeinsames Verfahren) des Hessischen Datenschutzgesetzes (HDSG) in der Fassung vom 07.01.1999 (GVBl. I S. 98),	Erlass des Hessischen Ministeriums des Innern und für Landwirtschaft, Forsten und Naturschutz (StAnz. 1999 S. 1226)

E-Health-Gesetz (SdKGWG)	Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze i. d. F. vom 21.12.2015 (BGBl. I S. 2408)
Entscheidung 2004/915/EG der EU-Kommission zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer	vom 27.12.2004, Az. K(2004) 5271 (ABl. L 385/74)
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz) vom 07.07.2005 (BGBl. I S. 1970, 3621), zuletzt geändert durch Artikel 311 der Verordnung vom 31. August 2015 (BGBl. I S. 1474)
EU-DSGVO-Entwurf	Entwurf für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutz-Grundverordnung) vom 15.12.2015, in englischer Fassung (EN) , Council oft he European Union (15039/15)
FATCA-USA-UmsV	Verordnung zur Umsetzung der Verpflichtungen aus dem Abkommen zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten und hinsichtlich der als Gesetz über die Steuerehrlichkeit bezüglich Auslandskonten bekannten US-amerikanischen Informations- und Meldebestimmungen i. d. F. vom 23.07.2014 (BGBl. I S. 1222)
GewO	Gewerbeordnung i. d. F. vom 22.02.1999 (BGBl. I S. 202), zuletzt geändert durch Artikel 275 der Verordnung vom 31.08.2015 (BGBl. I S. 1474)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) vom 13.08.2008 (BGBl. I S. 1690), zuletzt geändert durch Verordnung vom 31.08.2015 (BGBl. I S. 1474)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 07.01.1999 (GVBl. I S. 98), zuletzt geändert durch Gesetz vom 16.12.2015 (GVBl. I S. 594)
HGB	Handelsgesetzbuch i. d. F. vom 10.05.1897 (RGBl. I S. 219 zuletzt geändert durch Gesetz vom 20.11.2015 (BGBl. I S. 2029)
HHG, HE	Hessisches Hochschulgesetz i. d. F. vom 14.12.2009 (GVBl. I S. 666), zuletzt geändert durch Gesetz vom 30.11.2015 (GVBl. S. 510)
HKJGB	Hessisches Kinder- und Jugendhilfegesetzbuch (Kinderförderungsgesetz) i. d. F. vom 18.12.2006 (GVBl. I S. 698), zuletzt geändert durch Gesetz vom 28.09.2015 (GVBl. S. 366)
HSchG	Hessisches Schulgesetz i. d. F. vom 14.06.2005 (GVBl. I S. 441),

	geändert durch Gesetz vom 18.12.2012 (GVBl. I S. 645) 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 28.12.2015 (GVBl. I S. 346)
IntNutzRL,HE	Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung (StAnz. 2012 S. 526)
IT-Sicherheitsgesetz	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme i. d. F. vom 17.07.2015 (BGBl. I S. 1324)
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz) i. d. F. vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Gesetz vom 20.11.2015 (BGBl. I S. 2029)
MiLoG	Gesetz zur Regelung eines allgemeinen Mindestlohns (Mindestlohngesetz) i. d. F. vom 11.08.2014 (BGBl. I S. 1348)
OWiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 13.05.2015 (BGBl. I S. 706)
Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/58/EG	vom 25.11.2009 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Cookie-Richtlinie) (ABl. L 337/11)
Safe-Harbor-Abkommen der EU-Kommission	Entscheidung der EU-Kommission 2000/520/EG vom 26.07.2000 (ABl. L 215/7)
Safe-Harbor-Entscheidung des EuGH	Entscheidung des EuGH C-362/14 vom 06.10.2015, die das Safe-Harbor-Abkommen zwischen Europa und den USA für ungültig erklärt hat
Schengen-Evaluierungsverordnung (EU) des Rates Nr. 1053/2013	vom 07.10.2013 zur Einführung eines Evaluierungs- und Überwachungsmechanismus für die Überprüfung der Anwendung des Schengen-Besitzstands und zur Aufhebung des Beschlusses des Exekutivausschusses vom 16.09.1998 bezüglich der Errichtung des Ständigen Ausschusses Schengener Durchführungsübereinkommen (ABl. L 295/27)
SdKGWG (E-Health-Gesetz)	Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze i. d. F. vom 21.12.2015 (BGBl. I S. 2408)
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil – i. d. F. vom 11.12.1975 (BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 18.01.2015 (BGBl. I S. 2325)
SGB II	Sozialgesetzbuch Zweites Buch – Grundsicherung für Arbeitsuchende – i. d. F. vom 13.05.2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 24.06.2015 (BGBl. I S. 974)
SGB IV	Sozialgesetzbuch Viertes Buch – Gemeinsame Vorschriften für die Sozialversicherung – i. d. F. vom 12.11.2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), zuletzt geändert durch Gesetz vom 20.11.2015 (BGBl. I S. 2010)
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche

	Krankenversicherung – i. d. F. vom 20.12.1988 (BGBl. I S. 2477, 2482) zuletzt geändert durch Gesetz vom 01.12.2015 (BGBl. I S. 2114)
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe – i. d. F. vom 11.09.2012 (BGBl. I S. 2022), zuletzt geändert durch Gesetz vom 28.10.2015 (BGBl. I S. 1802)
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz – i. d. F. vom 18.01.2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 11.08.2014 (BGBl. I S. 1348)
StGB	Strafgesetzbuch i. d. F. vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 10.12.2015 (BGBl. I S. 2218)
StromGVV	Verordnung über Allgemeine Bedingungen für die Grundversorgung von Haushaltskunden und die Ersatzversorgung mit Elektrizität aus dem Niederspannungsnetz (Stromgrundversorgungsverordnung) vom 26.10.2006 (BGBl. I S. 2391), zuletzt geändert durch Verordnung vom 22.10.2014 (BGBl. I S. 1631)
StVG	Straßenverkehrsgesetz i. d. F. vom 05.03.2003 (BGBl. I S. 310, 919), geändert durch Gesetz vom 08.06.2015 (BGBl. I S. 904)
TMG	Telemediengesetz i. d. F. vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 17.07.2015 (BGBl. I S. 1324)
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) vom 17.12.1992 (BGBl. 1993 I S. 2), zuletzt geändert durch Gesetz vom 22.12.2011 (BGBl. I S. 2959
Vorschlag für Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (EU-Richtlinie für Justiz und Inneres/JI-RL)	vom 25.01.2012, Verfahren 2012/0010/COD [KOM(2012) 10 endg.]
WEG	Wohnungseigentumsgesetz vom 15.03.1951 (BGBl. I S. 175), zuletzt geändert durch Gesetz vom 05.12.2014 (BGBl. I S. 1962)

Kernpunkte

1. Die EU-Datenschutzreform (Datenschutz-Grundverordnung und JI-Richtlinie) befand sich im Berichtsjahr 2015 im abschließenden Trilog zwischen EU-Parlament, Kommission und Ministerrat. Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben die Verhandlungen verfolgt und mit eigenen Stellungnahmen, Positionspapieren und Gesprächen gegenüber den Trilogpartnern Einfluss genommen (Ziff. 1.2, 1.2.1, 1.2.2, 7.3, 7.11).

2. Der EuGH erklärte am 06.10.2015 die Safe-Habor-Entscheidung der Kommission für ungültig. Damit entzog der EuGH allen Transfers von personenbezogenen Daten in die USA, die sich bislang auf die Kommissionsentscheidung gestützt haben, die Rechtsgrundlage. Neue Instrumentarien sind erforderlich. Bis dahin sind von den Aufsichtsbehörden datenschutzrechtliche Maßnahmen im Einzelfall zu treffen (Ziff. 1.3, 7.5, 9.1).

3. Für die Verfahren bei Zuverlässigkeitsprüfungen, der Aufzeichnung eingehender Notrufe sowie dem Einsatz von Body-Cams bei der Polizei wurden durch die Novellierung des HSOG datenschutzrechtlich akzeptable Rechtsgrundlagen geschaffen (Ziff. 3.1.1).

4. Mit der Novellierung des Hessischen Hochschulgesetzes wurde u.a. die gesetzliche Grundlage für ein Forschungsinformationssystem geschaffen (Ziff. 3.1.2, 3.4.1).

5. Auch der Hessische Datenschutzbeauftragte unterliegt der Auskunftspflicht gemäß § 18 HDSG (Ziff. 3.1.4).

6. Die digitale Verwaltung kommt voran: Als erstes Bundesland ermöglicht Hessen die datenschutzgerechte, elektronische Antragsstellung mittels Einsatz des neuen Personalausweises (eID-Funktion) für Fördermittel nach dem Bundesausbildungsförderungsgesetz (BAföG) und dem Gesetz zur beruflichen Ausbildungsförderung (AFBG); (Ziff. 3.2.1).

7. Beim Postversand von Daten, die einem erhöhten Schutzbedürfnis unterliegen, kann der vollelektronische Versand mittels E-Post-Brief der Deutschen Post AG genutzt werden, wenn die Daten in einer verschlüsselten Form übermittelt werden (Ziff. 3.3.2). Entsprechendes gilt auch für den E-Mail-Versand. Maßnahmen zur

Transportverschlüsselung müssen z. B. von Finanzunternehmen eingesetzt werden, die Finanzinformationen von Kunden per E-Mail versenden (Ziff. 4.4.2).

8. Videoüberwachung ist nur in begrenztem Rahmen zulässig. Im Einzelfall können technische Maßnahmen wie Verpixelung oder Ausblenden zu datenschutzkonformen Anwendungen führen. Kamera-Attrappen unterliegen nach der Rechtsprechung nicht dem Anwendungsbereich des BDSG (Ziff. 4.9).

9. Smart-TVs, die für internetbasierte Dienste genutzt werden können, lassen unter Umständen Rückschlüsse auf das Verhalten der Nutzer zu. Sind die Dienste bereits standardmäßig werkseitig aktiviert, wird dieser Umstand dem Nutzer oft nicht bewusst. Zudem sind Smart-TVs zunehmend Ziele von Hackerangriffen. Hier gilt es, auf die Anbieter einzuwirken, dass sie dem Datenschutz größere Bedeutung schenken (Ziff. 5.3, 5.4).

10. Auskunfteien dürfen personenbezogene Daten zum Zwecke der Auskunftserteilung nicht unbegrenzt speichern. Das BDSG gibt vor, unter welchen Bedingungen die Daten wieder zu löschen sind (Ziff. 4.3.1). Dies gilt auch für die Daten von Vereinsmitgliedern zur Erstellung von Mitgliedspässen (Ziff. 4.2) sowie für die Aufbewahrung von Besucherdaten der Spielbanken (Ziff. 4.4.9).

11. Die Einwilligung einer Person in eine Datenverarbeitung kann nur dann als Rechtsgrundlage dienen, wenn die Einwilligung informiert und freiwillig erfolgt. Zur Information gehört es, dem Einwilligenden die gesamte geplante Datenverarbeitung transparent zu machen, zur Freiwilligkeit gehört, jeglichen Aufbau einer Drucksituation für den Betroffenen zu unterlassen. Dies gilt für alle Lebensbereiche, z. B. bei Klinikfragebogen (Ziff. 4.8.2), bei der Verarbeitung von Daten in einem Anamnesebogen einer Blutspendeeinrichtung (Ziff. 4.8.1), bei Bürgerbefragungen (Ziff. 3.3.6) und bei der Bereitstellung von digitalen Haushaltsbüchern durch Banken (Ziff. 4.4.4).

12. Kreditinstitute sind nach dem FATCA-USA-Umsetzungsabkommen verpflichtet, eine Kundenbeziehung auf eine mögliche USA-Steuerpflicht zu überprüfen. Sofern eine US-Steuerpflicht angenommen werden kann, ist eine Datenübermittlung über das Bundeszentralamt für Steuern an die Bundessteuerbehörden der Vereinigten Staaten von Amerika zulässig (Ziff. 4.4.3).

13. Unternehmen, deren Auskunftstätigkeit sich auf die Überprüfung und Ermittlung von Anschriften beschränkt, haben die Regelungen des BDSG zu beachten, die für die gewerbliche Datenverarbeitung zum Zwecke der Übermittlung gelten (Ziff. 4.3.3). Dies gilt auch für Unternehmen, die als Reseller ihre Leistungen unter Nutzung der Leistungen einer Auskunftei erbringen (Ziff. 4.3.4).

14. Im Onlinehandel ist es unzulässig, vor der Auswahl einer für den Onlinehändler risikobehafteten Zahlungsart durch den Kunden eine Bonitätsauskunft einzuholen. Betreiber von Onlineshops, die Bonitätsabfragen nur zur kundenfreundlichen Gestaltung ihres Workflows durchführen, müssen mit aufsichtsrechtlichen Maßnahmen rechnen (Ziff. 4.3.6.2).

15. Bei der Videoidentifizierung durch Banken nach dem Geldwäschegesetz sind datenschutzrechtliche Anforderungen zu beachten, die nicht von allen im Markt verfügbaren Produkten standardmäßig unterstützt werden. Die Nutzung des Dienstes Skype ist unzulässig (Ziff. 4.4.5).

16. Der Einsatz einer an der Windschutzscheibe eines Pkw installierten Videokamera ist datenschutzrechtlich nur unter engen Voraussetzungen zulässig. Bei Unzulässigkeit kann ein Bußgeldbescheid erlassen werden (Ziff. 4.1.3).

17. Die von mir schon lange vertretene Rechtsauffassung zur zulässigen Speicherung von Kontoauszügen in Leistungsakten der Sozialbehörde zum Bezug von Hartz IV wurde im Berichtszeitraum durch zwei Landessozialgerichte bestätigt (Ziff. 6.3).

18. Nach wie vor fehlt es nach Ansicht der Datenschutzbehörden des Bundes und der Länder an der Umsetzung der sog. Cookie-Richtlinie der EU durch den Bundesgesetzgeber. Nutzer müssen sich selbst informieren und ggfs. Abwehrmaßnahmen treffen, wenn sie die Verfolgung ihres Internet-Verhaltens ausschließen wollen (Ziff. 5.6, 7.1).

19. Bei der Betreuung von Flüchtlingen durch ehrenamtliche Helfer können in vielerlei Hinsicht datenschutzrechtliche Fragestellungen auftreten. Betroffen sind sowohl Daten der Helfer als auch Daten der Flüchtlinge. Hier gilt es, der Sondersituation entsprechenden Datenschutz zu gewährleisten (Ziff. 3.3.3).

20. Nach einer Vielzahl von unberechtigten Zugriffen auf eine Krankenakte im Jahr 2014 entwickelt das Klinikum Offenbach ein neues Zugriffskonzept für sein Krankenhausinformationssystem (Ziff. 4.8.6.).

1. Einführung

1.1
Allgemeines

Der Berichtzeitraum war geprägt durch die europäische und internationale Entwicklung des Datenschutzrechts. Während die europäische Datenschutzreform Fortschritte machte, verschärften sich die Schwierigkeiten bei der transatlantischen Übermittlung personenbezogener Daten in die USA. Die europäische und globale Entwicklung des Datenschutzrechts bestimmte maßgeblich auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, deren turnusmäßiger Vorsitz im Berichtszeitraum dem Land Hessen oblag.

1.2
Die europäische Datenschutzreform

Die europäische Datenschutzreform, die mit den Vorschlägen der europäischen Kommission vom 25.01.2012 für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr [Datenschutz-Grundverordnung – KOM(2012)11 endg.] sowie für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr [JI-Richtlinie – KOM(2012)10 endg.] als Paket in Angriff genommen worden war, wurde auch im Jahr 2015 fortgeführt.

1.2.1
EU-Datenschutz-Grundverordnung

Nach der heftigen Kritik, auf die der Kommissionsvorschlag gestoßen war, hatte das Europäische Parlament in seinem Standpunkt vorgeschlagen, den Kommissionsvorschlag in folgenden Kernpunkten zu ergänzen: territorialer Anwendungsbereich, Einwilligung in die Datenverarbeitung, Recht auf Löschung, Benachrichtigungspflichten, standardisierte Informationspolitiken, Datenportabilität, Profiling, Datentransfer, Kontrollzuständigkeiten und

Sanktionen. Damit waren zahlreiche Kritikpunkte entfallen. Weil aber die ursprünglich angenommenen Datenschutzaspekte der Verordnung von der zuständigen Arbeitsgruppe der EU in großen Teilen abgeändert worden waren, kam es erneut zu massiver Kritik. So forderten 66 unabhängige Verbraucher- und Datenschutzorganisationen *Jean-Claude Juncker* im April 2015 auf, den "Gold-Standard des europäischen Datenschutzes" zu erhalten. Umgekehrt sollte nach einem Positionspapier der Arbeitsgruppe der Industrie das Sammeln von personenbezogenen Daten ohne festgelegte Zwecke ebenso wie die Weitergabe dieser Daten an Dritte erlaubt werden. Vorbereitet durch die Arbeitsgruppe "Informationsaustausch und Datenschutz" (DAPIX) und durch den Ausschuss der Ständigen Vertreter (AStV) erörterte der Rat den Vorschlag der Kommission und die Ergänzungen des Parlaments. Nach langen Verhandlungen wurde der Vorschlag des Parlaments zunächst vom Rat abgelehnt. Am 15.06.2015 einigten sich jedoch die europäischen Innen- und Justizminister auf eine allgemeine Ausrichtung zur Datenschutz-Grundverordnung. Die Einigung betraf unter anderem folgende Punkte:

– Stärkung der Betroffenenrechte: Die Verordnung stärkt das Recht auf „Vergessenwerden“; unter bestimmten Voraussetzungen muss der Verantwortliche die Daten löschen. Durch das Recht auf Datenübertragbarkeit wird es für die Bürger leichter werden, personenbezogene Daten zwischen Diensteanbietern zu übertragen. Der Verantwortliche muss in klarer und einfacher Sprache genaue Informationen darüber geben, was mit den personenbezogenen Daten geschieht.

– Fairer Wettbewerb: Auch Unternehmen, deren Sitz außerhalb der EU liegt, müssen die Regelungen der Verordnung beachten, wenn sie Dienstleistungen in der EU anbieten. In bedeutenden grenzüberschreitenden Fällen, die Datenschutzaufsichtsbehörden in mehreren EU-Staaten betreffen, wird eine einheitliche Aufsichtsentscheidung getroffen.

– Zentrale Anlaufstellen: Unternehmen müssen sich nur noch an eine Datenschutzaufsichtsbehörde wenden und nicht mehr mit Aufsichtsbehörden in mehreren Mitgliedstaaten kommunizieren. Das Gleiche gilt für Bürger: Auch sie können sich an die nationale Datenschutzbehörde ihres Mitgliedstaates und in ihrer Sprache wenden, selbst wenn die Datenverarbeitung außerhalb ihres eigenen Mitgliedstaates erfolgt.

– Höhere Geldbußen: Die für die Verarbeitung von Daten Verantwortlichen können, wenn sie die Datenschutzvorschriften missachten, mit Geldbußen von bis zu 10 Mio. EUR

oder 2 % ihres gesamten Jahresumsatzes, bei schweren Verstößen bis zu 20 Mio. EUR oder 4 % des gesamten Jahresumsatzes, belegt werden.

Mit der allgemeinen Ausrichtung wurde zugleich das Mandat zum Trilog erteilt, der am 24.06.2015 von EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung *Vera Jourová* gemeinsam mit dem Verhandlungsführer des EU-Parlaments und den Justizministern der künftigen und vergangenen Ratspräsidentschaften gestartet wurde. Vor der Schlussabstimmung war noch streitig, wie Verstöße gegen die Verordnung geahndet werden sollen, ob Nutzer „eindeutig" oder „ausdrücklich" in die Verarbeitung ihrer personenbezogenen Daten einwilligen müssen und unter welchen Bedingungen Daten später für Big Data-Analysen genutzt werden dürfen. Am 15.12.2015 erzielten Rat, Parlament und Kommission eine Einigung (Ratsdokument 15039/15). Mit dieser Einigung wurde der Forderung des Rates entsprochen, die Verhandlungen über die Datenschutzreform bis Ende 2015 abzuschließen. Die formelle Schlussabstimmung ist im Frühjahr 2016 vorgesehen.

1.2.2
EU-Richtlinie für Justiz und Inneres

Das Datenschutzrecht im Bereich des Sicherheitsrechts (Polizei und Justiz) war deutlich weniger reguliert als die sonstigen Verwaltungsbereiche. Der Rahmenbeschluss 208/977/JI galt nur für den grenzüberschreitenden Datenverkehr. Die Datenschutzreform sieht auch für diesen Bereich gravierende Änderungen vor. Die Reform nahm ihren Fortgang durch die allgemeine Ausrichtung des Rats am 08.10.2015 (Ratsdokument 12555/15). Nach fünf Trilogen, die vom Oktober 2015 an stattgefunden haben, erzielten die Gesetzgebungsorgane Einvernehmen zu einem Gesamtkompromisstext. Damit können die Datenschutz-Grundverordnung und die JI-Richtlinie als Gesamtpaket verabschiedet werden. Die beiden Handlungsrahmen schließen sich wechselseitig aus, ihre Abgrenzung dürfte noch erhebliche Schwierigkeiten bedeuten.

1.3
Safe Harbor

Die Übermittlung personenbezogener Daten ist ein wesentliches Element der transatlantischen Beziehungen. Die EU und die USA sind wechselseitig die wichtigsten

Handelspartner. Handelsbeziehungen erfordern unverzichtbar den Austausch auch von personenbezogenen Daten. Allerdings verfügen die USA im Allgemeinen über kein als angemessen anerkanntes Datenschutzniveau, was einem ungehinderten Datenaustausch im Wege stand. Um Datentransfers aus den Mitgliedstaaten der EU in die USA zu erleichtern, erließ die Europäische Kommission auf der Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46/EG (EU-Datenschutzrichtlinie) am 26.07.2000 die sogenannte Safe-Harbor-Entscheidung (200/520/EG). Nach dieser galten solche US-Unternehmen, die sich den Safe-Harbor-Prinzipien per Selbstzertifizierung unterworfen hatten, als „sicherer Hafen“, so dass Daten weitgehend ungehindert dorthin fließen können. Der EuGH erklärte am 06.10.2015 die Safe-Harbor-Entscheidung der Kommission für ungültig (Urteil des Gerichtshofs der Europäischen Union vom 06.10.2015, C-362/14; http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5a2cb28ee3dd740419315c0addf82ec00.e34KaxiLc3eQc40LaxqMbN4ObNyNe0?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=100547); Unternehmen dürfen seit diesem Tag keine Daten mehr allein auf der Grundlage von Safe Harbor in die USA übermitteln.

Der EuGH stützt seine Entscheidung vor allem auf formale Argumente. Unter anderem wird ausgeführt, dass die Safe-Harbor-Entscheidung die Spielräume der nationalen Datenschutzaufsichtsbehörden, Transfers auf der Grundlage von Safe Harbor zu untersagen, zu stark einschränkt.

Trotz ihrer von Anfang an geäußerten Kritik an der Safe-Harbor-Entscheidung (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf; WP 32 der Artikel 29-Datenschutzgruppe m.w.N., zuletzt Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA“, in diesem Bericht zitiert unter Ziff. 7.5) gingen die Datenschutzaufsichtsbehörden in der EU bis zu dem Urteil des EuGH davon aus, grundsätzlich an die Entscheidung der Europäischen Kommission, Safe Harbor schaffe ein angemessenes Datenschutzniveau, gebunden zu sein. Der EuGH machte jedoch deutlich, dass auch die nationalen Datenschutzaufsichtsbehörden das Recht und die Pflicht haben, die Rechte der betroffenen Personen auch dadurch sicherzustellen, dass eine eigene Bewertung des Datenschutzniveaus für solche Länder außerhalb der EU angestellt wird, in die die Daten der Betroffenen fließen sollen.

Darüber hinaus hielt es der EuGH für erforderlich, Negativkriterien zu benennen, die einer Entscheidung, in einem Land herrsche ein angemessenes Datenschutzniveau, im Wege

stehen. Hierzu zählt, dass eine Vorratsdatenspeicherung ohne Differenzierung des Ziels dieser Speicherung sowie der Zugriffe auf so gespeicherten Daten stattfindet ebenso wie das Fehlen von Rechtsbehelfen, die es dem Betroffenen ermöglichten, Zugang zu den zu seiner Person gespeicherten Daten zu erhalten und diese berichtigen oder löschen lassen zu können.

Die Datenschutzaufsichtsbehörden der EU sind nunmehr gehalten, selbst anhand dieser Kriterien zu prüfen, ob ein Transfer personenbezogener Daten in die USA rechtmäßig ist. Dies gilt in jedem Fall für sämtliche Datenexporte in solche Länder der Erde, für die die Europäische Kommission eine sogenannte Angemessenheitsentscheidung nach Artikel 25 der EU-Datenschutzrichtlinie getroffen hat. Inwieweit sich die allgemeinen Ausführungen des Gerichts auch auf solche Transfermechanismen nach Artikel 26 der EU-Datenschutzrichtlinie [Standardvertragsklauseln, BCR, sogenannte Ad-hoc-Verträge, aber auch die Ausnahmen nach Art. 26 Abs. 1 EU-Datenschutzrichtlinie (Einwilligung etc.)] auswirken, wird derzeit von den Datenschutzaufsichtsbehörden in Deutschland und der EU geprüft. Der HDSB beteiligt sich hieran intensiv sowohl auf deutscher als auch auf EU-Ebene.

1.4
Bericht über das Jahr – Vorsitz der Datenschutzkonferenz

Im Jahr 2015 war ich Vorsitzender der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (seit dem 01.10.2015: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder).

Auf dem Europäischen Datenschutztag 2015 am 28.01.2015 in Berlin übernahm ich den Vorsitz von meinem Hamburger Kollegen Prof. Dr. J. Caspar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist ein Zusammenschluss von 18 Mitgliedern. Ihr gehören an der Bund und die 16 Bundesländer, wobei Bayern aufgrund verwaltungsorganisatorischer Besonderheiten zwei Vertreter schickt, die gemeinsam eine Stimme haben. Die 16 Bundesländer und der Bund sind untereinander gleichgestellt.

Das Vorsitzland hat im Vorsitzjahr in der Regel die Aufgabe, eine Frühjahrs- und eine Herbstkonferenz auszurichten. Die Frühjahrskonferenz wurde am 18./19.03.2015 in Wiesbaden durchgeführt, die Herbstkonferenz fand am 30.09.2015 und 01.10.2015 in

Darmstadt statt. Die dabei getroffenen Entschließungen sind unter Ziff. 7.2 bis 7.9, 7.12 und 7.13 abgedruckt.

Hierbei hatte es aber nicht sein Bewenden. Das Vorhaben der Konferenz, sich eine Geschäftsordnung zu geben, und die aktuellen Entwicklungen in Europa machten es dringend erforderlich, rund um die Themen Arbeitsweise der Konferenz, Europäische Datenschutz-Grundverordnung, das EuGH-Urteil zu Safe Harbor und die JI-Richtlinie eine Reihe von Sondertreffen der Konferenz zu organisieren und durchzuführen.

Am 24.06.2015 tagte die Datenschutzkonferenz in Kassel in den Räumen des Regierungspräsidiums. Die Sonderkonferenz befasste sich damit, die Geschäftsordnung für die Datenschutzkonferenz zu formulieren.

Auf diesen Termin folgten zwei weitere Sondersitzungen in Frankfurt, die am 22.08.2015 (Frankfurt I) und am 18.09.2015 (Frankfurt II) stattfanden. Die Konferenz Frankfurt I befasste sich mit dem Thema Ablauf des Kohärenzverfahrens sowie der Kooperation der Datenschutzbeauftragten im Lichte der Datenschutz-Grundverordnung. Die aufgeworfenen Fragen wurden in dem zweiten Sondertreffen der Datenschutzkonferenz (Frankfurt II) bearbeitet.

Nach der Herbstkonferenz in Darmstadt ergab sich infolge des Safe-Harbor-Urteils des EuGH in Sachen Schrems weiterer Bedarf für eine Zusammenkunft der Datenschutzkonferenz. Diese tagte am 21.10.2015 in Frankfurt (Frankfurt III). Auf Grundlage der in einer Arbeitsgruppensitzung am 09.10.2015 in Hannover erarbeiteten Erkenntnisse sowie der Ergebnisse der Artikel 29-Gruppe am 15.10.2015 wurde das weitere gemeinsame Vorgehen der Datenschutzkonferenz nach dem Safe-Harbor-Urteil des EuGH beraten und in einem Positionspapier (s. Ziff. 9.1) festgehalten.

Meine Teilnahme an der International Privacy Conference Amsterdam 2015 diente der Wahrnehmung der Interessen der Datenschutzkonferenz.

Als ein Ergebnis fand am 16.11.2015 ein Workshop mit dem Europäischen Datenschutzbeauftragten (EDPS) in der Hessischen Landesvertretung statt. Der EDPS äußerte den Wunsch, die Mitglieder der Konferenz kennenzulernen und mit ihnen gemeinsam die mit dem Inkrafttreten der DSGVO auf Europa und Deutschland im Speziellen zukommenden neuen Aufgaben und Herausforderungen zu erörtern. Ein weiterer Fokus des EDPS lag auf der Kooperation der Länder im Bereich Datenschutz.

Um das Thema „Safe Harbor“ und die Debatte darum zu vertiefen, habe ich Julie Brill, Mitglied der US-Bundeshandelskommission (Federal Trade Commission/FTC), nach Berlin zu einem Gespräch mit der Datenschutzkonferenz eingeladen. Die Konferenz traf sich am 08.12.2015 mit der FTC-Commissioner in Berlin.

Unter meinem Vorsitz hat sich die Datenschutzkonferenz 2015 erneut gegenüber der Datenschutz-Grundverordnung positioniert. Aus Anlass des Trilogs zur Datenschutz-Grundverordnung erstellte die Konferenz ein weiteres Positionspapier (s. Ziff. 9.1). Es wurde ins Englische übersetzt und der Öffentlichkeit bei einem Termin am 26.08.2015 in der Bundespressekonferenz vorgestellt.

Mit diesem Trilogpapier ist eine Delegation der Datenschutzkonferenz unter meiner Leitung nach Brüssel gefahren und hat am 31.08.2015 und 16.09.2015 Gespräche mit Vertretern des EU-Rates, der EU-Kommission und des EU-Parlaments in Brüssel geführt.

Mit der Sondersitzung Frankfurt IV am 27.01.2016 und der Planung und Durchführung des Europäischen Datenschutztages am 28.01.2016 wird ein arbeits- und erfolgreiches Konferenzjahr durch die Übergabe des Vorsitzes an Mecklenburg-Vorpommern zu Ende gehen.

1.5
Arbeitsschwerpunkte

Der Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) bildete in diesem Jahr einen erheblichen arbeitsintensiven Schwerpunkt (s. Ziff. 1.4). In diesem Zusammenhang waren zwei zweitägige Hauptkonferenzen (Wiesbaden, Darmstadt), sechs eintägige Sonderkonferenzen bzw. Sondertreffen (drei in Frankfurt, eine in Kassel und zwei in Berlin) zu den Themen Datenschutz-Grundverordnung und Safe Harbor und je ein Gesprächstermin einer Delegation der DSK mit Vertretern der EU-Kommission, dem EU-Rat und dem EU-Parlament zu organisieren, durchzuführen und nachzubereiten.

Mit Prüfungen im Bereich von Auskunfteien und Inkassounternehmen sowie Kommunen wurden vermehrt auch anlasslose, eigeninitiierte Kontrollen durchgeführt (s. Ziff. 4.3.2, 4.3.7, 3.3.1).

Gleichwohl überwogen im Berichtszeitraum wieder die Bearbeitung von Eingaben und Beratungsanfragen sowie die Durchführung anlassbezogener Prüfungen vor Ort.

Nach wie vor komplex sind Eingaben und Beratungen zum internationalen Datenverkehr. Die Entscheidung des EuGH zu Safe Harbor (s. Ziff. 1.3.) hat die Situation noch verschärft. Unternehmen reagieren verunsichert und irritiert auf die Entscheidung. Im Berichtsjahr 2015 gab es zu diesem Thema daher erheblichen Auskunfts- und Beratungsbedarf.

Im Übrigen zeigte die Intensität der Eingaben ein ähnliches Bild wie im Vorjahr.

1.6
Statistik

In der nachstehend aufgeführten Tabelle sind die Ergebnisse der automatisierten Auswertung unseres Dokumentverwaltungssystems nach Anzahl der Eingaben und Beratungsanfragen dargestellt.

Sie enthält nicht die Zahl der Eingaben und Anfragen, die mich telefonisch erreichten und auch telefonisch erledigt wurden, ohne dass sie einen Niederschlag in Akten gefunden haben. Da dies einen ebenfalls nicht zu vernachlässigenden Aufwand verursacht, wurden – wie in den Jahren zuvor – diese Telefon-Fälle für den Monat November als Stichprobe gezählt und für das Jahr hochgerechnet.

Arbeitsstatistik des Hessischen Datenschutzbeauftragten

Dokumentierte Eingaben

Fachgebiet	Anzahl
Auskunfteien und Inkassounternehmen	230
Wohnen, Miete und Nachbarschaft	283
Elektronische Kommunikation	167
Werbung und Adresshandel	89
Kreditwirtschaft, Spielbanken, Lotto	87
Beschäftigtendatenschutz	112
Polizei, Justiz, Strafvollzug und Gerichte	86
Soziales	100
Gesundheitswesen	134
Schulen und Hochschulen, Archive, Bibliotheken, Museen	124
Verkehr und Daseinsvorsorge, Geodaten	92
Kommunen	112
Handel und Handwerk	53
Versicherungen	33
Vereine und Verbände	26

Rundfunk, Fernsehen, Presse	20
Forschung, Planung und Statistik	21
Sonstiges	21
Technik und IT-Sicherheit	22
Summe der dokumentierten Eingaben	**1.812**
Summe der dokumentierten Beratungsanfragen	**281**
davon Eingaben und Beratungen Videoüberwachung betreffend	369
Summe der telefonischen Eingaben und Beratungen	**4.824**
Gesamtsumme	**6.917**

Die bereits in den Vorjahren festgestellte Tendenz, wonach Beratungen sich in aller Regel deutlich aufwändiger gestalten als die Bearbeitung von Eingaben, hat sich erneut bestätigt. Anscheinend binden Unternehmen die Aufsichtsbehörde im Vorfeld datenschutzrelevanter Entscheidungen eher ein. Viele Anfragen kommen auch von betrieblichen Datenschutzbeauftragten für ihre Mandanten bzw. Unternehmen. Das begrüße ich, zum einen zeigt diese Entwicklung auf, dass Datenschutzbewusstsein vermehrt in den Unternehmen vorhanden ist, zum anderen ist die rechtzeitige Einbindung der Aufsichtsbehörde letztendlich sinnvoller und kostengünstiger als nachträglich – z. B. aufgrund einer Beschwerde oder Kontrolle – Konsequenzen ziehen zu müssen.

Im Berichtszeitraum beschäftigten mich auch wieder Ordnungswidrigkeitenverfahren (Ziff. 4.1).

Auch in diesem Jahr musste ich von der Möglichkeit Gebrauch machen, einen Strafantrag gemäß § 44 Abs. 2 BDSG zu stellen.

Die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG führte zu 87 Meldungen. Nach jeweiliger Prüfung stellte sich heraus, dass von den angezeigten Vorfällen 62 Meldungen tatsächlich solche waren, in denen eine Pflicht zur Information der Aufsichtsbehörde bestand.

2. Europa

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 2015 dar.

Um die Koordination der Aufsicht für das Schengener Informationssystem der zweiten Generation (SIS II) sicherzustellen, treffen sich die Vertreter der nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte (EDSB) zweimal jährlich. Vertreten sind die nationalen Datenschutzbehörden der 28 EU-Mitgliedstaaten. Darüber hinaus gehören die nationalen Datenschutzbehörden Islands, Liechtensteins, Norwegens und der Schweiz zu dieser Gruppe, da ihre Länder auch an diesem System teilnehmen. Den Vorsitz der Gruppe hat derzeit die portugiesische Datenschutzbehörde, den stellvertretenden Vorsitz die maltesische Datenschutzbehörde inne.

Wichtig aus deutscher Sicht war die Behandlung des Problems der Ausschreibungen von gestohlenen oder sonst abhandengekommenen Kraftfahrzeugen (s. 43. Tätigkeitsbericht, Ziff. 2.4.1). Darüber hinaus fand in diesem Jahr in Deutschland ein Vor-Ort-Evaluierungsverfahren durch Sachverständige statt, um zu überprüfen, ob Deutschland die Schengen-Bestimmungen korrekt umsetzt und anwendet.

2.1.1
Ausschreibungen von gestohlenen Kraftfahrzeugen im SIS II

Im 43. Tätigkeitsbericht (Ziff. 2.4.1) hatte ich das Problem der im SIS II ausgeschriebenen Kraftfahrzeuge für deutsche Kraftfahrzeughalter dargelegt. Der Erwerber eines Kraftfahrzeugs, das im SIS II als gestohlen oder abhandengekommen ausgeschrieben ist, sieht sich rechtlichen und praktischen Schwierigkeiten ausgesetzt, z. B. beim Versuch des Weiterverkaufs oder bei Reisen innerhalb des Schengen-Raums. Die Frage ist, ob die zugrundeliegende Ausschreibung gelöscht werden kann, wenn das Fahrzeug gefunden wurde, oder ob es weiterer Voraussetzungen für die Löschung bedarf. Die Kontrollgruppe hat

das Thema in der Sitzung der ersten Jahreshälfte erneut aufgegriffen und umfassend diskutiert.

Die Auslegung des Art. 38 des Beschlusses 2007/533/JI war dabei weiterhin Gegenstand der Diskussion.

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;

…

Während einige Delegationen, so auch meine Mitarbeiterin, die Auffassung vertraten, mit dem Auffinden des Kraftfahrzeugs sei der Zweck der Ausschreibung erfüllt und eine Löschung der Ausschreibung erforderlich, waren andere Delegationen der Meinung, eine solch strikte Interpretation der Vorschrift sei nicht angezeigt. Ein praxistauglicher Ansatz sei zu bevorzugen, der den beteiligten nationalen Stellen eine Handlungsempfehlung aufzeigt. Daher versuchte die Kontrollgruppe, unabhängig von den nationalen Einzelfällen und von den rechtlichen Fragen, einen gemeinsamen Ansatz zu finden, um mit den praktischen Problemen im Zusammenhang mit der (zu löschenden) Ausschreibung umzugehen.

Die Delegationen stimmten darin überein, dass eine fortdauernde Speicherung über mehrere Jahre zu Rechtsunsicherheit führe und für den Betroffenen, d. h. für den Kraftfahrzeughalter, nicht zumutbar sei. Auf der anderen Seite dürfe nicht bereits das bloße Auffinden des Kraftfahrzeugs zu einer Löschung führen. Es müsse ein Mittelweg gefunden werden, um die Interessen aller Beteiligten zu einem Ausgleich zu bringen. Es bedarf folglich insofern – darin sind sich die Delegationen einig – eines verbindlichen Maßnahmenkatalogs, der die einzelnen Schritte und Verantwortlichkeiten festlegt und von den Mitgliedstaaten beachtet wird. Sobald sich die beteiligten Mitgliedstaaten über das Vorgehen in dem betreffenden Einzelfall anhand des Katalogs verständigt haben, kann die Ausschreibung gelöscht werden. Über die Einzelheiten eines solchen Maßnahmenkatalogs wird in den künftigen Sitzungen noch beraten werden. Soweit die Delegationen übereinstimmen, wird es eine offizielle

Stellungnahme der Kontrollgruppe zu dem Problem der Ausschreibungen geben. Hiermit ist im kommenden Jahr zu rechnen.

2.1.2
Schengen-Evaluierung in Deutschland

Auf der Grundlage des mehrjährigen Evaluierungsprogramms für den Zeitraum 2014 bis 2019 wurde vom EU-Rat im Oktober 2014 das Evaluierungsprogramm für das Jahr 2015 genehmigt. Die turnusmäßige Schengen-Evaluierung Deutschlands im Bereich „Datenschutz“ fand im Juni/Juli des Berichtszeitraums statt. Infolge des Inkrafttretens der Schengen-Evaluierungsverordnung (EU) Nr. 1053/2013 sind die Mitgliedstaaten nicht mehr alleine, sondern gemeinsam mit der Europäischen Kommission für die Evaluierung zuständig. Eine europäische Evaluierungskommission, bestehend aus Experten der EU-Mitgliedstaaten und Vertretern der Europäischen Kommission, besuchte vom 28.06.2015 bis zum 03.07.2015 unter anderem das Bundeskriminalamt, das Bundesinnenministerium sowie die Bundespolizei.

Die Experten prüfen bei dem Vor-Ort-Besuch, ob die EU-Mitgliedstaaten die datenschutzrechtlichen EU-Grundlagen im Bereich des Schengener Besitzstandes korrekt anwenden. Zur Behebung gegebenenfalls festgestellter Mängel bzw. zur Optimierung der Anwendung können in einem abschließenden Prüfbericht konkrete Empfehlungen an den evaluierten Schengen-Staat ausgesprochen werden. Der geprüfte Staat muss anschließend Maßnahmenpläne erstellen und der zuständigen EU-Rats-Arbeitsgruppe über deren Umsetzung regelmäßig berichten. Meine Mitarbeiterin nahm neben Vertretern der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) an Gesprächen mit der Evaluierungskommission teil. Der endgültige Bericht der Expertengruppe über den Prüfbesuch in Deutschland lag im Berichtszeitraum noch nicht vor.

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 vier Sitzungen in Brüssel sowie

an Treffen der Arbeitsgruppe "Neue Projekte" teilgenommen. Der Beitrag stellt die Arbeitsschwerpunkte im Jahr 2015 dar.

2.2.1
Neue Rechtsgrundlage für Europol

Über die geplante neue Rechtsgrundlage für Europol und die verschiedenen Stellungnahmen der Gemeinsamen Kontrollinstanz (GKI) wurde bereits im 41. Tätigkeitsbericht (Ziff. 3.1.2), 42. Tätigkeitsbericht (Ziff. 3.1.4.3) und 43. Tätigkeitsbericht (Ziff. 2.5.1) berichtet.

Der Kommissionsentwurf [COM(2013) 173 endg.] ist im Berichtszeitraum weiter überarbeitet worden. Sowohl unter lettischer als auch unter luxemburgischer Präsidentschaft wurden eine Reihe von Trilogverhandlungen zwischen Europäischer Kommission, Rat und Europäischem Parlament geführt. Ende Juni d. J. fand ein Gespräch mit dem Berichterstatter für den Entwurf für eine Europol-Verordnung im Europäischen Parlament, Herrn Diaz de Mera, und verschiedenen Mitgliedern der GKI statt.

Das vorrangige Thema dieses Gesprächs war die datenschutzrechtliche Kontrolle von Europol. Dabei geht es um die Frage, in welchem Ausmaß die nationalen Datenschutzbehörden in den Mitgliedstaaten an der Kontrolle beteiligt werden. Dies ist deshalb so wichtig, weil der größte Teil der bei Europol verarbeiteten Daten aus den Mitgliedstaaten stammt. Auch sollten die Kenntnisse über die Datenverarbeitung bei Europol und die Erfahrungen, die die Mitglieder der Kontrollgruppe im Laufe der Zeit gewonnen haben, nicht verloren gehen, sondern weiterhin für die Kontrolle erhalten bleiben.

Alle bisherigen Textfassungen gehen davon aus, dass der Europäische Datenschutzbeauftragte (EDPS) für die Kontrolle zuständig ist. Während der Entwurf der Kommission sich darauf beschränkt, die Zusammenarbeit zwischen EDPS und nationalen Aufsichtsbehörden zu regeln, sieht die Allgemeine Ausrichtung des Rats (Rat der Europäischen Union 28.05.2014, 10033/14) einen Beirat für die Zusammenarbeit (Cooperation Board) mit den nationalen Aufsichtsbehörden und dem EDPS vor. Nach letzterem Vorschlag würden die nationalen Aufsichtsbehörden der Mitgliedstaaten stärker in die Kontrolle eingebunden, sie hätten zum Beispiel das Recht gegenüber dem EDPS über spezielle Fragen unterrichtet zu werden oder auch Mitspracherechte bei Entscheidungen des EDPS auszuüben, die ihre Mitgliedstaaten betreffen. Im Fall der Mitsprache ist vorgesehen,

dass der EDPS – falls er dem Standpunkt des betroffenen Mitgliedstaates in einer konkreten Frage nicht folgt – den Beirat für die Zusammenarbeit damit befasst.

Die GKI machte in ihrem Gespräch deutlich, dass sie aus den schon genannten Gründen einen Beirat mit möglichst weitgehenden Kompetenzen für die Zusammenarbeit favorisiert. Seitens des Berichterstatters wurde darauf verwiesen, dass die Entscheidung über das Kontrollmodell noch nicht abschließend getroffen sei. Vieles spricht dafür, dass zunächst die Verabschiedung des Entwurfs für eine JI-Richtlinie [Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Untersuchung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr KOM(2012) 10 endg.] abgewartet wird, um die Europol-Verordnung darauf abzustimmen.

2.2.2
Stellungnahme zur Verarbeitung von Daten über Personen, die Opfer von Menschenhandel sind

Sowohl bei verschiedenen Kontrollen, die die GKI bei Europol durchgeführt hat, als auch bei Kontrollen von nationalen Datenschutzaufsichtsbehörden der Mitgliedstaaten gab es immer wieder Probleme mit der Verarbeitung von Daten von Opfern im Bereich des Menschenhandels. Diese beruhen zum Teil darauf, dass die Grenzen zwischen Täter- und Opferstatus oftmals fließend sind bzw. beide Eigenschaften auf eine Person zutreffen können. So ist es zum Beispiel typisch für diese Art von Kriminalität, dass eine Person eine Straftat begeht, zu dieser aber als ein Opfer von Menschenhandel gezwungen wird. Zudem können verschiedene Behörden an der Strafermittlung und -verfolgung beteiligt sein, die den Status Täter oder Opfer unterschiedlich bewerten.

Die GKI hat deshalb u. a. gefordert, dass alle an der Ermittlung und Verfolgung von Straftaten beteiligten Behörden in der Europäischen Union die gleichen Kriterien verwenden, um eine Person als Opfer einzustufen. Dafür sollten die Behörden schon bestehende Listen mit Indikatoren benutzen, die bei der Einstufung einer Person als Opfer hilft (z. B. Handbuch des Büros der Vereinten Nationen für Drogen- und Verbrechensbekämpfung für die Bekämpfung des Menschenhandels für Praktiker aus der Strafjustiz, UN.GIFT, Global Initiative to Fight Human Trafficking, www.unodc.org). Die GKI hat weiter dargelegt, dass

eine Person zunächst auch in den Fällen als Opfer und nicht als Täter eingeordnet werden soll, wenn nicht ausgeschlossen werden kann, dass sich der Opferstatus später ändert.

2.2.3
Liste der am meisten gesuchten Personen

Die Arbeitsgruppe “Neue Projekte“ der GKI, in der meine Mitarbeiterin vertreten ist, hat sich u. a. mit dem Vorhaben von Europol befasst, 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. Deutschland gehört zu den Staaten, die eine derartige Liste nicht führen.

Die Mitglieder der Arbeitsgruppe sind der Auffassung, dass eine derartige Liste mangels gesetzlicher Grundlage nicht bei Europol betrieben werden kann, wenn davon auszugehen ist, dass Europol selbst diese Daten verarbeitet. Die Datenverarbeitung müsste vielmehr durch die Mitgliedstaaten erfolgen. Derzeit wird an einer technischen Lösung gearbeitet, wie das nachvollziehbare Interesse von Europol an einer derartigen Liste realisiert werden kann.

3. Datenschutz im öffentlichen Bereich

3.1
Landesverwaltung

3.1.1
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Im HSOG wurden langjährige Forderungen des Datenschutzes umgesetzt – die Schaffung einer Rechtsgrundlage für Zuverlässigkeitsüberprüfungen sowie für die Aufzeichnung von Notrufen bei der Polizei. Mit weiteren Änderungen wurden die Voraussetzungen für den Einsatz der Body-Cams erheblich erweitert, deren Auswirkungen müssen in der Praxis beobachtet werden.

Im Zusammenhang mit der notwendigen Reform des Landesmeldegesetzes hat der Gesetzgeber auch einige nicht unwesentliche Änderungen im HSOG beschlossen. Ich hatte Gelegenheit im Rahmen einer öffentlichen Anhörung im Innenausschuss zu diesem Vorhaben Stellung zu nehmen. Nicht in allen Punkten wurden meine Anregungen berücksichtigt.

Aus Sicht des Datenschutzes waren drei Änderungen bzw. Ergänzungen im HSOG relevant:
– Zuverlässigkeitsüberprüfungen
– Aufzeichnung von Telekommunikationsdaten
– Erweiterung der Einsatz-Möglichkeiten der Body-Cam.

3.1.1.1
Beteiligung der Polizei an Zuverlässigkeitsüberprüfungen

Die Rechtmäßigkeit von sogenannten Zuverlässigkeitsüberprüfungen auf Grundlage einer Einwilligung der Betroffenen war schon lange Gegenstand der Erörterungen zwischen dem Innenministerium und mir. Erstmals im größeren Rahmen wurden solche Überprüfungen im Kontext großer Veranstaltungen aus Anlass der Fußball-Weltmeisterschaft 2006 durchgeführt. Gleichzeitig gab es solche Überprüfungen aber auch in nicht unerheblichem Umfang für Personen, die in bestimmten (sicherheitsempfindlichen) Bereichen tätig sein

wollten – etwa bei der Polizei oder in einer Justizvollzugsanstalt. Dies betraf sowohl (zukünftige) Bedienstete als auch Personen, die etwa als Handwerker oder als Putzkräfte dort tätig sein sollten.

Bedenken gegen diese Verfahrensweise hatte ich aus zwei Gründen: Soweit (zukünftige) Arbeitnehmer betroffen sind, ist es mehr als fraglich, ob eine Einwilligung in die für die Überprüfung notwendige Datenverarbeitung wirklich freiwillig erfolgt. Nur eine solche kann aber grundsätzlich eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sein, soweit nicht eine ausdrückliche rechtliche Regelung vorliegt. Hinzu kommt, dass es nach meiner Einschätzung grundsätzlich auch nicht zulässig ist, die Aufgaben der Polizei als Eingriffsverwaltung auf der Grundlage von Einwilligungen zu erweitern.

Andererseits konnte auch ich mich nicht in allen Fällen den formulierten Sicherheitsbedenken verschließen. Deshalb habe ich es begrüßt, dass nunmehr für solche „Zuverlässigkeitsüberprüfungen“ eine ausdrückliche Rechtsgrundlage geschaffen wurde.

Auch der Ansatz – zwischen Überprüfungen zum Schutz staatlicher Einrichtungen und Veranstaltungen sowie von besonderen Veranstaltungen außerhalb des öffentlichen Bereichs zu differenzieren – ist meines Erachtens sachgerecht.

§ 13a HSOG

(1) Soweit das Hessische Sicherheitsüberprüfungsgesetz oder ein anderes Gesetz keine Sicherheitsüberprüfung vorsieht, können die Polizeibehörden Personen einer Zuverlässigkeitsüberprüfung unterziehen, die

1. eine Tätigkeit als Bedienstete anstreben
   a) in einer Behörde mit Vollzugsaufgaben,
   b) in einer anderen öffentlichen Stelle, bei der sie regelmäßig Zugriff auf Personalaktendaten von Bediensteten haben, die bei einer Behörde mit Vollzugsaufgaben verwendet werden oder
   c) in besonders gefährdeten Liegenschaften öffentlicher Stellen,
2. selbstständige Dienstleistungen zur Unterstützung von Vollzugsaufgaben erbringen wollen,
3. unbegleiteten Zutritt zu Liegenschaften von Behörden mit Vollzugsaufgaben oder Liegenschaften öffentlicher Stellen, die besonders gefährdet sind, erhalten sollen, ohne den in Nr. 1 und 2 genannten Personengruppen anzugehören,

4. Zugang zu Vergabe- und Vertragsunterlagen haben, aus denen sich sicherheitsrelevante Funktionszusammenhänge, insbesondere aus baulichen und betrieblichen Anforderungen für Liegenschaften der Polizei oder der Justiz, ergeben, oder
5. die Zulassung zum Besuch von Gefangenen oder Untergebrachten in einer Justizvollzugseinrichtung begehren.

Eine Zuverlässigkeitsüberprüfung kann ferner durchgeführt werden bei Personen, für die ein privilegierter Zutritt zu einer Veranstaltung einer Behörde oder öffentlichen Stelle beantragt wird.

(2) Die Polizeibehörde kann die Identität der Person feststellen, deren Zuverlässigkeit überprüft werden soll, und zu diesem Zweck von ihr vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern. Die Überprüfung erfolgt mit Einwilligung der betroffenen Person anhand von Datenbeständen der Polizeien des Bundes und der Länder, im Fall von Erkenntnissen über Strafverfahren auch der Justizbehörden und Gerichte. Für die Einwilligung gilt § 7 Abs. 2 des Hessischen Datenschutzgesetzes mit der Maßgabe, dass die Erklärung stets der Schriftform bedarf. Der betroffenen Person ist zudem mitzuteilen, wo sie weitere Auskünfte zu dem Verfahren erhalten kann und dass sie sich gleichfalls an den Hessischen Datenschutzbeauftragten wenden kann.

(3) Entscheidet die für die Überprüfung zuständige Polizeibehörde nicht zugleich auch über die Zuverlässigkeit, unterrichtet sie die ersuchende Stelle darüber, ob sicherheitsrelevante Erkenntnisse vorliegen, gegebenenfalls durch Angabe von

1. Deliktsbezeichnung,
2. Tatort,
3. Tatzeit,
4. Ausgang des Verfahrens, soweit feststellbar, sowie
5. Name und Aktenzeichen der sachbearbeitenden Justiz- oder Polizeibehörde.

Bei anderen als Gefahrenabwehr- und Polizeibehörden sowie Justizbehörden beschränkt sich die Rückmeldung auf die Auskunft, ob Sicherheitsbedenken vorliegen. Der Datenaustausch kann in einem gemeinsamen Verfahren nach Maßgabe des § 15 des Hessischen Datenschutzgesetzes stattfinden.

(4) In den Fällen des Abs. 1 Satz 1 Nr. 2 bis 5 sowie Satz 2 sind mit Einwilligung der betroffenen Person Wiederholungsüberprüfungen zulässig, wenn seit der letzten

Überprüfung mindestens ein Jahr vergangen ist und kein Grund zu der Annahme besteht, dass die Voraussetzungen des Abs. 1 nicht mehr vorliegen. Wiederholungsüberprüfungen können in den Fällen des Abs. 1 Satz 2 auch in Bezug auf gleichartige Veranstaltungen durchgeführt werden. Werden Wiederholungsüberprüfungen auf Ersuchen durchgeführt, unterrichtet die ersuchende Behörde die Polizeibehörde über den Wegfall der Voraussetzungen des Abs. 1.

(5) Nach Abschluss der Überprüfung speichert die Polizeibehörde die Verfahrensunterlagen zu Dokumentationszwecken bis zum Ende des Jahres, das dem Jahr des Abschlusses folgt. Finden Wiederholungsüberprüfungen statt, dürfen die Unterlagen auch für diesen Zweck verarbeitet werden; sie sind bis zum Ende des Jahres zu speichern, das der Abmeldung oder der Feststellung der fehlenden Zuverlässigkeit folgt.

(6) Die Befugnisse nach § 13 Abs. 1 Nr. 2 bis 4, Abs. 2 sowie den §§ 14 bis 26 bleiben unberührt.

§ 13b HSOG

(1) Eine Zuverlässigkeitsüberprüfung kann durchgeführt werden bei Personen, für die ein privilegierter Zutritt zu einer besonders gefährdeten Veranstaltung in nicht öffentlicher Trägerschaft beantragt wird. Die Polizeibehörde hört den Hessischen Datenschutzbeauftragten an, wenn eine Zuverlässigkeitsüberprüfung nach Satz 1 beabsichtigt ist.

(2) § 13a Abs. 2, 5 und 6 dieses Gesetzes sowie § 15 des Hessischen Datenschutzgesetzes gelten entsprechend. Die Rückmeldung an einen Empfänger außerhalb des öffentlichen Bereichs beschränkt sich auf die Auskunft zum Vorliegen von Sicherheitsbedenken. Sie darf von diesem nur für die Entscheidung verarbeitet werden, ob der überprüften Person der privilegierte Zutritt gewährt werden soll. Der Empfänger teilt der Polizeibehörde mit, wenn er der Empfehlung nicht folgt. Er hat alle von ihm für die Zuverlässigkeitsüberprüfung erhobenen Daten spätestens bei Beendigung der Veranstaltung zu löschen.

Zwar stellt sich auch weiterhin die Frage, ob die im Gesetz vorgesehene „Einwilligung“ in die Überprüfung die Voraussetzungen für eine wirksame Einwilligung in eine Datenverarbeitung erfüllt. Denn in aller Regel wird diese allein deshalb erfolgen, da ansonsten eine Tätigkeit im

gewünschten Bereich nicht möglich ist, was u. a. auch Konsequenzen für ein bestehendes Arbeitsverhältnis haben könnte. Andererseits ist durch dieses Verfahren sichergestellt, dass den Betroffenen diese Überprüfung transparent ist – was in der derzeitigen Praxis nicht immer der Fall ist. Durch die direkte Beteiligung besteht zumindest die Möglichkeit von sich aus auf eine entsprechende Tätigkeit zu verzichten oder ggf. auch rechtzeitig vorher noch weitere Argumente vorzutragen, warum trotz vorhandener Erkenntnisse eine positive Entscheidung zur Zuverlässigkeit erfolgen könnte. Deswegen habe ich meine grundsätzlichen Bedenken zur Möglichkeit einer freiwilligen Einwilligung, insbesondere im Arbeitsverhältnis, in diesem Kontext zurückgestellt.

Das vom Gesetz beschriebene Verfahren entspricht der Vorgehensweise bei solchen Zuverlässigkeitsüberprüfungen, die schon länger gesetzlich geregelt sind, etwa für den Bereich der Luftsicherheit.

Schließlich gibt es eine klare Festlegung der Zweckbindung der in diesem Kontext zu erhebenden Daten. Dies gilt sowohl für die bei der Polizei im Rahmen der Überprüfung, aber auch für die bei einem Arbeitgeber anfallenden Informationen.

Die Vorgaben des § 13b HSOG, dass es sich um besonders gefährdete öffentliche Veranstaltungen handeln muss, sowie dass ich vorab zu hören bin, können bei sachgerechter Behandlung dazu dienen, dass die Zahl der Anwendungsfälle begrenzt ist. Inwieweit dies gelingt, muss die zukünftige Praxis zeigen. Ich werde jedenfalls sorgfältig unter Beachtung des Verhältnismäßigkeitsgrundsatzes im Einzelfall abwägen, ob eine solche Überprüfung – und auch für welchen konkreten Personenkreis – wirklich notwendig ist.

3.1.1.2
Aufzeichnung von Notrufen

Auf die Notwendigkeit zur Schaffung einer gesetzlichen Grundlage für die Aufzeichnung der Telekommunikation bei der Polizei habe ich schon länger hingewiesen. Die gesetzliche Grundlage ist erforderlich, da jegliches Aufzeichnen von Anrufen einen Eingriff in das durch Art. 10 GG geschützte Telekommunikationsgeheimnis darstellt.

Die nunmehr getroffene Regelung sichert im Wesentlichen die bisherige Praxis. Neben der Aufzeichnung der klassischen Notrufe unter Nutzung der Rufnummer 110 kann auch die Aufzeichnung anderer Gespräche notwendig sein. Dies gilt zum einen, soweit ein „Notruf“

über eine andere Rufnummer bei der Polizei eingeht. Es kann sich aber auch im Laufe eines Gesprächs ein Grund herausstellen, der die Notwendigkeit der Dokumentation des Wortlautes des Gesprächs begründet. Das kann etwa für Fälle gelten, in denen Straftaten angekündigt werden, oder Gespräche, in deren Verlauf Drohungen ausgesprochen werden.

Da es sich nicht nur bei der Aufzeichnung selbst um einen Eingriff in das Telekommunikationsgeheimnis handelt, sondern auch die spätere Verwendung der so erhobenen Daten einen erneuten Eingriff darstellt (vgl. BVerfGE 100, 313), sind klare Regelungen zur Verwendung dieser Daten notwendig, die insbesondere den Grundsatz der Verhältnismäßigkeit wahren.

Die nunmehr verabschiedete Regelung entspricht dem.

§ 20 Abs. 11 HSOG

Die Polizeibehörden zeichnen Notrufe und Meldungen über sonstige Notrufeinrichtungen sowie den Funkverkehr ihrer Leitstellen auf. Gefahrenabwehr- und Polizeibehörden können sonstige Telekommunikation aufzeichnen, wenn dies für ihre Aufgabenerfüllung erforderlich ist; auf die Aufzeichnung soll hingewiesen werden, soweit dadurch die Aufgabenerfüllung nicht gefährdet wird. Soweit erforderlich, können die Aufzeichnungen

1. zur Abwehr einer Gefahr,
2. zur Strafverfolgung oder
3. zur Dokumentation behördlichen Handelns

verarbeitet werden. Aufzeichnungen sind spätestens nach drei Monaten zu löschen, wenn sie nicht zu einem Zweck nach Satz 3 verarbeitet werden.

Im Gesetzentwurf war auch noch die Verwendung der aufgezeichneten Daten zur Verfolgung von Ordnungswidrigkeiten vorgesehen. Dies hätte den Verhältnismäßigkeitsgrundsatz nicht gewahrt.

Aus der Begründung des Entwurfs (LTDrucks. 19/1979, S. 37) ließ sich zwar eine gewisse Einschränkung entnehmen – so sollte die Verwendung dann erfolgen dürfen, wenn der Anruf selbst einen Ordnungswidrigkeitstatbestand verwirklicht. Gedacht sei insoweit an ähnliche Sachverhalte wie der Missbrauch von Notrufeinrichtungen oder (strafbare) Äußerungen im Rahmen des Gesprächs, die als Begründung für die Verwendung der Aufzeichnungen zur Strafverfolgung benannt waren. Der Wortlaut der Norm enthielt jedoch keinerlei

Einschränkungen. Mir war auch nicht ersichtlich, welche Ordnungswidrigkeitstatbestände hier hätten in Betracht kommen könnten.

Als Ergebnis der Anhörung im Innenausschuss wurde dann auch dieser Vorschlag aus dem Text gestrichen.

3.1.1.3
Erweiterte Einsatzmöglichkeiten für die Body-Cams

Ich hatte im letzten Tätigkeitsbericht über den Modellversuch zum Einsatz der Body-Cams und die Diskussion zur erweiterten Anwendung dieser Technik sowie die Beschränkungen der Regelungen des § 14 Abs. 6 HSOG berichtet (43. Tätigkeitsbericht, Ziff. 4.1.2.1). Insbesondere aus Sicht der Anwender, aber auch in der allgemeinen politischen Diskussion wurde die Forderung laut, nicht nur Videoaufnahmen, sondern auch Tonaufzeichnungen zu ermöglichen. Ein in diesem Kontext häufig zu hörendes Argument war, dass nur so Beleidigungen der Polizisten dokumentiert werden könnten.

Darüber hinaus wurde diskutiert, inwieweit die technischen Möglichkeiten, die die eingesetzten Kameras bieten, für den Einsatz nutzbar sein könnten. Dies betraf das sogenannte Pre-Recording. Dabei wird das Videobild beim Einschalten der Pre-Recording-Funktion kontinuierlich auf ein flüchtiges Speichermedium mit begrenzter Speicherkapazität, wie den RAM-Speicher, abgelegt. Der Speicher wird durch Abschalten der Funktion oder durch Überschreiben späterer Sequenzen gelöscht. Sobald die Aufnahmefunktion des Kamerasystems eingeschaltet wird, kopiert das System die noch vorhandenen Daten des RAM-Speichers auf ein dauerhaftes Speichermedium, wie beispielsweise eine SD-Karte, und schreibt die neuen Videodateien direkt dahinter. Die zeitliche Begrenzung lässt sich variieren, die hessische Polizei plant in diesem Kontext eine Dauer von 30 Sekunden.

Dies soll eine verbesserte Dokumentation des Einsatzszenarios ermöglichen. So führte die Begründung des Gesetzentwurfes der Landesregierung aus (LTDrucks. 19/1979, S. 34):

„Die aus dem Pre-Recording gespeicherten Videodaten stehen dabei in sehr engem zeitlichem Zusammenhang mit der durch die Betätigung der Aufnahmefunktion der Body-Cam ausgelösten Aufzeichnung und umfassen lediglich einen kurzen Zeitraum. Die infolge der Pre-Recording-Funktion erhobenen personenbezogenen Daten tragen dazu bei, dass die Entstehung einer Situation und nicht nur das Handeln der Personen ab dem

Einschaltzeitpunkt dargestellt wird. Diese Videobilder bilden den Zeitraum und insbesondere auch die Umstände ab, die die Aufzeichnung zur Eigensicherung und zum Schutz dritter Personen erforderlich gemacht haben. Ohne die Verwendung der Pre-Recording-Funktion müssten die für die Eigensicherung der Polizeibeamten oder zum Schutz Dritter relevanten Situationen durch die eingesetzten Beamten jederzeit antizipiert und ein Einschalten der Aufnahmefunktion der Body-Cam durch diese so früh wie möglich angestrebt werden, um die Aufzeichnung zum erforderlichen Zeitpunkt im Sinne von § 14 Abs. 6 Satz 1 HSOG starten zu können. Damit erhöht sich die Wahrscheinlichkeit von Fehlaufnahmen, etwa weil sich die Situation doch nicht in der erwarteten Weise entwickelt hat. Durch das Pre-Recording können so die aufgrund der Aufzeichnung der Personen und ihrer Handlungen erfolgenden gerechtfertigten Eingriffe in das Recht auf informationelle Selbstbestimmung reduziert werden."

Beabsichtigt war zudem, die Einsatzmöglichkeiten von den Maßnahmen zur Identitätsfeststellung abzukoppeln. Es war beabsichtigt, dass eine Beobachtung schon zulässig sein sollte, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zum Schutz von Polizeibeamten erforderlich ist, d. h. im Vorfeld einer konkreten Gefahrensituation. Dies hätte die Einsatzschwelle deutlich herabgesenkt. Es wäre somit nicht ausgeschlossen, dass bei jeglichem polizeilichem Einsatz eine entsprechende Kamera mitgeführt wird.

Dies hätte den Rahmen der Verhältnismäßigkeit gesprengt. Schon allein das Mitführen einer Kamera ist geeignet, das Verhalten auch von Personen zu beeinflussen, die in keiner Weise von dem eigentlichen polizeilichen Einsatz tangiert sind. Da in der Praxis nicht ohne weiteres erkennbar ist, ob die Kamera aufzeichnet, erst recht nicht, ob die sogenannte Pre-Recording-Funktion aktiviert ist, wäre es für Passanten schwierig wahrzunehmen, ob sie möglicherweise von einer solchen Kameraaufzeichnung erfasst werden.

Diese Funktion kann auch nicht auf die Überlegungen des BVerfG aus der Entscheidung zur Kennzeichenerkennung im Urteil vom 11.03.2008 – 1 BvR 2074/05 u. a. – (BverfGE 120, 378 ff.) gestützt werden. Dort hatte das BVerfG ausgeführt, dass schon keine Datenerhebung stattfände, wenn lediglich eine technische Erfassung bzw. Verarbeitung der Daten erfolgt, weil der Abgleich unverzüglich erfolge und die Daten nicht ohne weitere Auswertung sofort und spurenlos gelöscht würden.

Unabhängig davon, dass je nach Kameraeinstellung schon die Frage, wie schnell nicht relevante Sequenzen gelöscht werden, einer Vergleichbarkeit entgegenstehen, entscheidet

bei der Pre-Recording-Funktion nicht allein die Technik, sondern der die Kamera bedienende Beamte, ob bestimmte Daten dauerhaft erfasst werden.

Nicht in allen Punkten ist der Landtag den Vorstellungen der Landesregierung in ihrem Gesetzentwurf gefolgt. Tonaufzeichnungen sind nunmehr zulässig. Ein dreistufiges Konzept in Form von “kurzfristiger technischer Erfassung“, “offener Beobachtung“ und “Aufzeichnung“, wobei sich die Anforderungen mit jeder Stufe erhöhen soll, eröffnet die Grundlage für die Nutzung der Pre-Recording-Funktion. Es bleibt jedoch bei der Koppelung an Maßnahmen im Kontext von Identitätsfeststellungen wie im bisherigen Rahmen.

§ 14 Abs. 6 HSOG

Die Polizeibehörden können an öffentlich zugänglichen Orten eine Person, deren Identität nach diesem Gesetz oder anderen Rechtsvorschriften festgestellt werden soll, mittels Bild- und Tonübertragung kurzfristig technisch erfassen, offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum Schutz von Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Dabei können personenbezogene Daten auch über dritte Personen erhoben werden, soweit dies unerlässlich ist, um die Maßnahme nach Satz 1 durchführen zu können. Sind die Daten für Zwecke der Eigensicherung oder der Strafverfolgung nicht mehr erforderlich, so sind sie unverzüglich zu löschen.

Es wird sich zeigen, ob die konkreten Einsätze diesen Anforderungen entsprechen und das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger gewahrt bleibt.

3.1.2
Stellungnahme des Hessischen Datenschutzbeauftragten zur Novellierung des Hessischen Hochschulgesetzes

Im Dezember 2014 hat mir das Hessische Ministerium für Wissenschaft und Kunst (HMWK) den Entwurf eines Gesetzes zur Änderung hochschulrechtlicher Vorschriften übermittelt und mir Gelegenheit gegeben, hierzu Stellung zu nehmen. Das habe ich in der Folge auch getan. Zwei Punkte hielt ich für regelungsbedürftig.

3.1.2.1
Qualitätssicherung und Berichtswesen

Die Hochschulen haben im Rahmen der Qualitätssicherung und Evaluation ein berechtigtes Interesse, eine Verbindung zu ihren ehemaligen Mitgliedern und Angehörigen aufzubauen und zu pflegen. Hierfür bedarf es einer gesetzlichen Grundlage, welche sich bislang weder im Hochschulgesetz noch in der Immatrikulationsverordnung wiederfand. Aus diesem Grund hatte ich vorgeschlagen, das Gesetz um folgende Passage zu ergänzen:

„Die Hochschulen dürfen personenbezogene Daten ihrer ehemaligen Mitglieder und Angehörigen nutzen, soweit dies ausschließlich zum Zwecke der Befragung im Rahmen der Qualitätssicherung und von Evaluationen oder zur Pflege der Verbindung mit diesen Personen erforderlich ist und diese nicht widersprechen. Die Befragten sind auf die Freiwilligkeit ihrer Angaben und die Möglichkeit zum Widerspruch der Nutzung hinzuweisen. Das Nähere regelt die Hochschule durch Satzung."

3.1.2.2
Gesetzliche Regelung zur Einführung von Forschungsinformationssystemen

Seit dem Jahr 2014 ist ein Verbund hessischer Hochschulen unter Federführung der Justus-Liebig-Universität Gießen darum bemüht, unter dem Namen HeFIS (Hessisches Forschungsinformationssystem) ein gemeinsames Informationssystem zu schaffen. Im Rahmen der Konzeption und Entwicklung eines derartigen Instrumentariums, bei dem z. B. personenbezogene Daten von Wissenschaftlerinnen und Wissenschaftlern der einzelnen Hochschulen einer breiten Öffentlichkeit zugänglich gemacht werden sollen, hat sich gezeigt, dass es an einer gesetzlichen Grundlage für die Datenverarbeitung mangelt, soweit sich die universitäre Einrichtung nicht durchgängig von der Einwilligung der Betroffenen abhängig machen will. Aus diesem Grund habe ich es für unabdingbar gehalten, eine gesetzliche Grundlage zu schaffen, welche einen Gestaltungsrahmen eröffnet, innerhalb dessen die Hochschulen kraft eigener Satzung die Inhalte und den Umfang des Informationssystems selbst festlegen können. Deshalb habe ich neben einer neuen Formulierung im Hochschulgesetz vorgeschlagen, die konkrete Ausgestaltung in eine allgemeinverbindliche Rechtsnorm (z. B. eine Rechtsverordnung) umzusetzen, die von den einzelnen Hochschulen durch die Verabschiedung einer Satzung ausgestaltet wird.

Folgenden Wortlaut hatte ich dem HMWK vorgeschlagen:

„Die Hochschulen können für sich selbst oder übergreifend im Verbund mit weiteren Hochschulen Forschungsinformationssysteme aufbauen und betreiben. Sie können zu diesem Zweck auch personenbezogene Daten erheben und verarbeiten. Das Nähere zu Umfang und Inhalt regelt eine Verordnung."

Das Ministerium hat in beiden von mir genannten Fällen meine Vorschläge berücksichtigt und in den Gesetzentwurf aufgenommen. Die Novelle des Hochschulgesetzes wurde im November 2015 vom Hessischen Landtag verabschiedet und ist zum 01.01.2016 in Kraft getreten.

3.1.3
Konkretisierung der E-Mail-Internet-Richtlinie der Landesverwaltung

Durch Eingaben wurde ich darauf aufmerksam gemacht, dass die E-Mail- und Internet-Richtlinie der Landesverwaltung einen Interpretationsspielraum eröffnet, wenn es darum geht die Gültigkeit einer E-Mail-Adresse zu prüfen. Hier bedarf es konkreter Vorgaben, um unzulässige Datenübermittlungen zu vermeiden.

Im letzten Jahr haben sich in verschiedenen Eingaben Probleme im Umgang mit E-Mails gezeigt. Gerade die konsequente Umsetzung der Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung (StAnz. 19/2012, S. 526 ff.) mit ihrer Vorgabe in Ziffer 2.1, 1. Satz: „grundsätzlich sollen alle Dokumente per E-Mail versandt werden, sofern nicht durch Rechtsvorschrift Schriftform vorgegeben ist", birgt Fallstricke.

In der Richtlinie ist nicht beschrieben, woran man die Identität des Absenders und damit bei einer Antwort des Empfängers festmachen kann. Auch gibt es keine Kriterien, um zu entscheiden, ob eine Adresse noch gültig ist.

Diese Schwierigkeiten sind bei der Nutzung von E-Mail allgegenwärtig. Wählt ein Kunde eine Mail-Adresse, gibt es in der Regel keine Einschränkungen, wenn diese noch nicht vergeben wurde. Es ist also möglich, sich zu einem fremden Namen eine Mail-Adresse zu verschaffen. Nicht zuletzt, um das zu verhindern, wurde die DE-Mail konzipiert. Um eine DE-Mail-Adresse zu erhalten, muss ein qualitativ hochwertiger Identifizierungsprozess durchlaufen werden. Die Maßnahmen sind aber nicht geeignet, eine unbefugte Kenntnisnahme zu verhindern,

wenn ein falscher Empfänger aus einer Liste ausgewählt wurde. In so einem Fall ist auch eine Verschlüsselung wirkungslos.

Es gab mehrere Eingaben, in denen Mails einen falschen Empfänger erreichten bzw. den richtigen Empfänger nicht erreichten.

Mit einer Behörde, bei der dieses Problem auftauchte, habe ich die Thematik diskutiert. Daraufhin hat man eine Anleitung erarbeitet und als Dienstanweisung verfügt, mit der nach meiner Auffassung die wesentlichen Fallstricke vermieden werden. Die Maßnahmen sind wie folgt:

1. E-Mail-Adressen unterliegen einem häufigen Wandel und oft werden Adressen gemeinsam mit anderen Personen geteilt. Die Information über die E-Mail-Adresse sollte deshalb nicht älter als sechs Monate sein. Die für dienstliche Kommunikation verwendeten Adressen sollen immer vom Adressaten selbst stammen und nur aus dem aktuellen diese Person oder diese Institution betreffenden behördlichen Vorgang entnommen werden. Eine Verwendung von Adressen aus anderen Vorgängen soll unterbleiben.

2. Wird die Behörde per E-Mail von Extern kontaktiert oder werden der Behörde bei der Kontaktaufnahme mehrere Kommunikationsadressen (Anschrift, E-Mail-Adresse, Telefonnummer) genannt, so können diese Adressen grundsätzlich genutzt werden.

3. Ohne vorherige Einwilligung des Absenders können technische Mitteilungen, allgemeine Auskünfte, Terminabstimmungen u. Ä. per unverschlüsselter E-Mail übermittelt werden. Allerdings gilt auch hier zu beachten, dass beispielsweise bei den Einträgen in die Betreffzeile keine vertraulichen Daten eingetragen werden sollen (Minimalprinzip).

4. Vertrauliche Daten dürfen nach Extern grundsätzlich nur verschlüsselt per E-Mail übermittelt werden. Da die Verschlüsselungstechnik nur wenig verbreitet ist, können mit Einwilligung der Kommunikationspartner auch vertraulich zu behandelnde Daten per E-Mail ausgetauscht werden. In diesen Fällen ist beim Absender nachzufragen und die Einwilligung zu dieser Kommunikationsform einzuholen. Die externen Partner sind dabei auf die Risiken und Gefahren einer offenen E-Mail-Kommunikation hinzuweisen. Hierfür soll folgender Standardtext verwendet werden:
   „Wenn Sie auch vertraulich zu behandelnde Daten in dieser Angelegenheit über unverschlüsselte E-Mail austauschen möchten, bitte ich hierzu um Ihre ausdrückliche

Einwilligung. Bei unverschlüsseltem E-Mail-Verkehr besteht grundsätzlich ein Risiko, dass unberechtigte Dritte Kenntnis vom Inhalt der Mitteilung erhalten könnten."

In der Regel ist dieses Vorgehen nur sinnvoll, wenn mit einer längeren wechselseitigen Kommunikation zu rechnen ist. Bei einer einmaligen Kontaktaufnahme ist standardmäßig die Rückantwort per Brief vorgesehen, wenn Zweifel über die Vertraulichkeit der Daten bestehen.

5. Bei besonders sensiblen Daten ist die Kommunikation mittels unverschlüsselter E-Mail auch bei Vorliegen einer Einwilligung ausgeschlossen. Bei diesen besonders geschützten Daten handelt es sich um Steuerdaten, Sozialdaten und den Katalog des § 7 Abs. 4 HDSG. Dies sind Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben. Bei diesen Daten hat die Kommunikation durch Brief zu erfolgen. Dies empfiehlt sich auch bei Zweifeln über die Kategorisierung der Angaben.

Darüber hinaus muss ein Bürger eine Antwort per Briefpost erhalten, wenn er es wünscht, auch dann, wenn die Anfrage selbst per E-Mail gestellt wurde.

Ich habe das HMDIS gebeten, bei der anstehenden Überarbeitung der o. g. Richtlinie diese aufgeführten Schwierigkeiten zu berücksichtigen und den Passus des grundsätzlichen Nutzungsgebots der E-Mail zu modifizieren.

3.1.4
Auskunftsansprüche nach § 18 HDSG gegenüber dem Hessischen Datenschutzbeauftragten

Auch der Hessische Datenschutzbeauftragte als oberste Landesbehörde ist eine öffentliche Stelle im Sinne des HDSG, so dass grundsätzlich auch ihm gegenüber das Recht auf Auskunft über die zu einer Person gespeicherten Daten besteht.

In diesem Jahr wurde ich mehrmals um Auskunft über die zu Petenten gespeicherten personenbezogenen Daten gebeten.

Der Hessische Datenschutzbeauftragte als eine oberste Landesbehörde ist selbstverständlich auch datenverarbeitende Stelle im Sinne des HDSG mit der Verpflichtung, die sich daraus ergebenden Vorgaben zum Umgang mit personenbezogenen Daten einzuhalten.

Damit ergibt sich auch ein Auskunftsanspruch für automatisiert gespeicherte Daten gem. § 18 Abs. 3 HDSG. Dieser umfasst die zu einer Person automatisiert gespeicherten Daten, Zweck und Rechtsgrundlage der Verarbeitung sowie – soweit dies gespeichert ist – die Herkunft und die Empfänger übermittelter Daten.

§ 18 Abs. 3 HDSG

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

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

In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden.

In meiner Dienststelle wird der Schriftverkehr in einem Registratursystem erfasst. Dieses enthält in elektronischer Form Postein- und -ausgänge sowie auch weitere Unterlagen, die im Rahmen der Bearbeitung einzelner Sachverhalte anfallen. Im Zusammenhang mit der Bearbeitung von Bürgereingaben gehören dazu in der Regel die Eingabe sowie ggf. zusätzliche Schreiben, meine Antworten an die Petenten, der Schriftwechsel mit den Stellen, gegen die sich die Eingabe richtet, sowie Vermerke der zuständigen Mitarbeiter.

Dies dient der ordnungsgemäßen Abwicklung des Schriftverkehrs sowie der Dokumentation des Verwaltungshandelns. Rechtsgrundlage ist § 11 i. V. m. § 24 HDSG. Das Registratursystem ersetzt nicht die Verwaltungsakte, diese wird weiterhin nicht automatisiert geführt.

Nicht alle Anfragen in diesem Kontext sind allerdings wirklich darauf gerichtet zu erfahren, welche Daten meine Dienststelle selbst verarbeitet.

Teilweise wird pauschal gefragt „ich bitte um Auskunft, welche Daten über mich (in Hessen) gespeichert sind“. Manche Anfragen sind auch konkreter, etwa die Bitte um Auskunft, welche Daten die Polizei speichert, oder auch Beschwerden über eine unzulässige Verarbeitung in einem Unternehmen, ohne dass klar ist, welche Daten dort verarbeitet werden.

In diesen Fällen weise ich die Petenten darauf hin, dass der Hessische Datenschutzbeauftragte zwar zur Kontrolle der datenverarbeitenden Stellen/Behörden in Hessen befugt ist. Der Auskunftsanspruch richtet sich aber konkret an die Stelle, die die Daten verarbeitet. Weder verfüge ich über ein Verzeichnis aller Datenverarbeitungssysteme in Hessen, noch habe ich einen Zugriff auf diese.

Soweit die Betroffenen näher ausführen, um welche Daten oder Stellen es geht, ist es auch möglich, konkretere Hilfsstellungen für ein Auskunftsersuchen zu geben. Dies kann etwa durch Hinweise auf die einschlägigen rechtlichen Voraussetzungen oder zu den notwendigen Angaben, um gespeicherte Daten der Person zuzuordnen, geschehen.

Vereinzelt gibt es schließlich Auskunftsersuchen im Anschluss an eine durch mich abgeschlossene Eingabe. Da das Auskunftsinteresse zu den eigenen Daten nicht begründet werden muss, ist der Grund für diese Anfragen nicht immer ersichtlich. Manche Petenten sind mit dem Ergebnis zu ihrer Eingabe nicht zufrieden und hoffen auf diesem Wege zusätzliche Informationen in der Sache zu bekommen. Manche wollen nähere Informationen über die konkreten sie betreffenden Vorgänge bei der datenverarbeitenden Stelle, über die sie sich beschwert haben.

Auskunft oder auch Akteneinsicht gem. § 18 Abs. 5 HDSG – ggf. auch durch Übersendung von Kopien – ist in diesen Fällen grundsätzlich dann möglich, wenn nicht berechtigte Interessen Dritter entgegenstehen.

§ 18 Abs. 5 HDSB

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der aktenführenden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. Werden die Akten nicht zur Person des Betroffenen geführt, hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig

großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach Abs. 3 zu erteilen. Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

Dass Schreiben von Behörden die Namen von Erstellern oder Ansprechpartnern enthalten, ist in der Regel kein Grund von der Auskunft abzusehen. Nur im Einzelfall kann beurteilt werden, ob der Inhalt eines Schreibens zur Auskunftsverweigerung führen muss. Neben Angaben zu anderen, an dem Verfahren beteiligten Personen kommt dies insbesondere in Betracht, soweit Geschäftsgeheimnisse betroffen sind oder wenn etwa dezidiert einzelne Maßnahmen der technischen Ausgestaltung der Datenverarbeitung – wie einzelne technische und organisatorische Sicherungsmaßnahmen – beschrieben sind.

Die Beschränkung meiner Möglichkeiten zur Auskunftserteilung gibt es schließlich auch noch in einem anderen Zusammenhang. § 18 Abs. 6 HDSG erlaubt datenverarbeitenden Stellen eine Auskunft ganz oder teilweise zu versagen, soweit besondere Geheimhaltungsinteressen vorliegen. Für Polizei und Verfassungsschutz gibt es vergleichbare Regelungen (§ 28 Abs. 3 bis 5 HDSG, § 18 HVerfSchG), die darüber hinaus auch die Möglichkeit eröffnen, von der Begründung für die Auskunftsverweigerung abzusehen, wenn sonst Rückschlüsse auf diese möglich sind.

§ 18 Abs. 6 HDSG

Abs. 1 und 3 gelten nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft der Leiter der verpflichteten Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass er sich an den Hessischen Datenschutzbeauftragten wenden kann.

§ 29 Abs. 3 bis Abs. 5 HSOG

(3) Abs. 1 gilt außerdem nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte der betroffenen Person hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung insoweit nicht, als durch die Mitteilung der Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

(5) Wird Auskunft nicht gewährt, ist die betroffene Person darauf hinzuweisen, dass sie sich an die Datenschutzbeauftragte oder den Datenschutzbeauftragten wenden kann. Dies gilt nicht in den Fällen des Abs. 1 Satz 4. Die Mitteilung der Datenschutzbeauftragten oder des Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern sie nicht einer weitergehenden Auskunft zustimmt.

§ 18 HVerfSchG

(1) Der betroffenen Person ist vom Landesamt für Verfassungsschutz auf Antrag gebührenfrei Auskunft über die zu ihrer Person gespeicherten Daten sowie den Zweck und die Rechtsgrundlage der Verarbeitung zu erteilen.

(2) Abs. 1 gilt nicht, soweit eine Abwägung ergibt, dass das Auskunftsrecht der betroffenen Person gegenüber dem öffentlichen Interesse an der Geheimhaltung der Tätigkeit des Landesamtes für Verfassungsschutz oder einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten muss. Ein Geheimhaltungsinteresse liegt dann vor, wenn

1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamtes für Verfassungsschutz zu befürchten ist,
3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen.

Die Entscheidung trifft der Behördenleiter oder ein von ihm besonders beauftragter Mitarbeiter.

(3) Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde. Die Gründe der Auskunftsverweigerung sind aktenkundig zu machen. Wird die Auskunftserteilung abgelehnt, ist die betroffene Person auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, dass sie sich an den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen des Hessischen Datenschutzbeauftragten dürfen keine Rückschlüsse auf den Erkenntnisstand des Landesamtes für Verfassungsschutz zulassen, sofern es nicht einer weitergehenden Auskunft zustimmt.

Meine Kontrollmöglichkeiten in diesem Kontext sind nicht beschränkt, allerdings kann ich nicht umfassend selbst Auskunft erteilen – weder durch detaillierte Wiedergabe meiner Erkenntnisse noch gar durch Einsicht in die in diesem Kontext bei mir geführten Akten. Andernfalls wäre es nicht ausgeschlossen, dass durch eine Auskunftserteilung eine berechtigte Auskunftsverweigerung der datenverarbeitenden Stelle umgangen würde. Das Recht, sich an den hessischen Datenschutzbeauftragten zu wenden, bezweckt nicht, eine Auskunftserteilung stellvertretend durch den Datenschutzbeauftragten zu ermöglichen. Sinn dieser Regelung ist die – dem Betroffenen hier nicht mögliche – Kontrolle der Rechtmäßigkeit der Datenverarbeitung.

In der Regel kann ich dem Betroffenen daher nur mitteilen, dass die Überprüfung ergeben hat, dass seine Rechte nicht verletzt sind und die datenverarbeitende Stelle die gesetzlichen Vorgaben im Kontext der Entscheidung über einen Auskunftsantrag eingehalten hat.

Wenn ich dann im Anschluss um Auskunft über die bei mir gespeicherten Daten bzw. um Akteneinsicht gebeten werde, muss auch ich dann im Sinne des § 18 Abs. 6 HDSG die Auskunft verweigern.

3.2
Sozialwesen

3.2.1
Hessisches BAföG-/AFBG-Verfahren

Bereits im 41. Tätigkeitsbericht (Ziff. 3.3.3.2) habe ich mich ausführlich mit dem Hessischen BAföG-/AFBG-Verfahren befasst. Das Verfahren wurde in den vergangenen Jahren unter meiner Begleitung weiterentwickelt. Es gehört heute durch die Möglichkeit, elektronisch mit Hilfe der eID-Funktion des neuen Personalausweises Anträge zu stellen, zu den modernsten in Deutschland.

3.2.1.1
Aktueller Sachstand

In meinem letztjährigen Tätigkeitsbericht hatte ich berichtet, dass im Jahr 2012 ca. 35.000 Antragsteller monatlich Zahlungen erhalten. Die Zahl der Berechtigten ist stark gestiegen. So wurden im Jahr 2014 in Hessen knapp 50.000 Studierende und 15.000 Schüler nach dem Bundesausbildungsförderungsgesetz (BAföG) mit zusammen etwa 224 Mio. EUR (Bundes- und Landesmittel) gefördert. Davon wurden 136 Mio. EUR in Form von Zuschüssen und 87 Mio. EUR in Form von Darlehen gewährt. Hinzu kamen knapp 9.000 Förderungen nach dem Gesetz zur Förderung der beruflichen Aufstiegsfortbildung (AFBG) in Höhe von insgesamt 32 Mio. EUR (Bundes- und Landesmittel), wovon zirka zwei Drittel als Darlehen vergeben wurden.

Die Antragsbearbeitung erfolgt in den fünf hessischen Studentenwerken und 26 kommunalen BAföG-Ämtern der hessischen Landkreise und kreisfreien Städte.

Im Mai 2012 wurde das aus den 1970er Jahren stammende und in den Studentenwerken eingesetzte IT-Großrechner- und Vorortverfahren durch das Hessische BAföG- und AFBG-Verfahren „HeBAV“ erfolgreich abgelöst. Gleichzeitig wurde HeBAV in den kommunalen BAföG-Ämtern eingeführt. Zeitgleich mit der Einführung wurde unter https://www.bafög-hessen.de die Möglichkeit einer Online-Beantragung geschaffen. Hessen bot dabei als erstes Bundesland die Möglichkeit, auf einer zentralen Plattform im Internet Mittel der Ausbildungsförderung für BAföG und AFBG zu beantragen. Antragstellende können dort jederzeit und mehrfach den Status der Bearbeitung online abfragen.

Im Februar 2014 hat Hessen – wiederum als erstes Bundesland – dieses Online-Angebot um die Möglichkeit erweitert, auch erforderliche Antragsunterlagen (Steuerbescheid der Eltern, Schulbescheinigungen von Geschwistern u. ä.) online in einen gesicherten Bereich hochzuladen und dort direkt an das für die Antragsbearbeitung zuständige Amt zu übermitteln. Der Status der Bearbeitung kann dabei, wie schon beim Antrag selbst, von den Antragstellenden ebenfalls online abgefragt werden.

Mit der funktionalen Erweiterung des hessischen „BAföG-Online-Portals“ um eine „Dokumenten-Upload-Möglichkeit“ verfolgt das Land Hessen das Ziel, die elektronische Antragstellung auszubauen und damit den Arbeitsaufwand bei der Bearbeitung von BAföG-Anträgen weiter zu reduzieren und insgesamt eine Reduktion der Bearbeitungszeit zu erwirken. Voraussetzung hierfür ist die Steigerung der Qualität eingereichter Anträge infolge einer elektronischen Plausibilitäts- und Vollständigkeitsprüfung bei der Online-Antragstellung, die zeitintensive Rückfragen vermindert, sowie die elektronische Zustellung und Zuordnung der sonstigen einzureichenden Dokumente, die den Weg über die Poststelle ablöst und somit die Bearbeitungszeiten weiter verkürzt. Dies hat eine schnellere Auszahlung von Förderungsleistungen an den Antragstellenden zur Folge.

Die Möglichkeit der Online-Antragstellung wurde im Jahr 2013 hessenweit von Studierenden für 10,52 % der BAföG-Erstanträge genutzt. Im Jahr 2014 stieg die Quote auf 13,81 % der BAföG-Erstanträge. Alternativ werden die für die Beantragung erforderlichen amtlichen Formblätter weiterhin in gedruckter Papierform angeboten. Diese können bei jedem Amt für Ausbildungsförderung angefordert oder abgeholt werden.

Durch das 25. BAföGÄndG wurden die Länder im Rahmen der Auftragsverwaltung durch Änderung des § 46 verpflichtet, „bis zum 01.08.2016 eine elektronische Antragstellung zu ermöglichen, die den Vorgaben des § 36a Abs. 2 Satz 4 Nr. 1 oder 2 des Ersten Buches Sozialgesetzbuch entspricht“. Das derzeit in Vorbereitung befindliche 3. AFBGÄndG sieht in § 19b eine vergleichbare Regelung vor. Den Antragstellenden soll dadurch ermöglicht werden, den Antrag vereinfacht online und „papierlos“ zu stellen und auf den bisher zwingend erforderlichen Prozess mit zusätzlichem Ausdruck, Unterschrift und Einreichung beim Amt zu verzichten.

Mit dem IT-Dienstleister des HMWK wurde nunmehr ein Konzept entwickelt, wie die durch das 25. BAföGÄndG vorgeschriebene Möglichkeit der elektronischen Antragstellung realisiert und mittels Einsatz des neuen Personalausweises (sog. eID-Funktion) nach § 21 des

Gesetzes über Personalausweise und elektronischen Identitätsnachweis umgesetzt werden kann. Die Softwareerweiterung ist fertig programmiert und einsatzfähig. Die Berechtigung, Daten im Wege des elektronischen Identitätsnachweises bei Inhabern des Personalausweises und elektronischen Aufenthaltstitels mittels eines Berechtigungszertifikates anzufragen, wurde von der zuständigen Vergabestelle des Bundesverwaltungsamtes erteilt.

Meine Behörde wurde beteiligt; die datenschutzrechtlichen Belange fanden Berücksichtigung, so dass keine datenschutzrechtlichen Bedenken gegen die vorgesehene Erweiterung bestehen.

Der Einsatz der sog. eID-Funktion ist nach Abschluss der geplanten Tests im November 2015 vorgesehen. Hessen wird mit dem Einsatz als erstes aller 16 Bundesländer neue Möglichkeiten bei der Online-Antragstellung für beide Leistungsgesetze eröffnen und die gesetzlichen Vorgaben weit vor dem gesetzlich vorgeschriebenen Datum (01.08.2016) erfüllen.
Zugleich wird es laut Auskunft des HMDIS auch in der gesamten hessischen Landesverwaltung der erste Einsatz der eID-Funktion sein. Das Ziel einer modernen, papierarmen und bürgerfreundlichen Verwaltung im Rahmen von E-Government und „Digitales Hessen 2020“ wird damit weiter gefördert.

3.2.2
Umgang mit der Schweigepflicht von Sozialarbeitern/Sozialarbeiterinnen oder Sozialpädagogen/Sozialpädagoginnen in einem Team der Kinder- und Jugendförderung

Im Bereich der Kinder- und Jugendarbeit kommt es immer wieder zu der Frage, in welchem Umfang ein fachlicher Austausch innerhalb eines Betreuungsteams über die Kinder und Jugendlichen erfolgen darf, ohne gegen (strafbewehrte) dienstliche Schweigepflichten zu verstoßen.

Städte beschäftigen häufig ein viele Personen umfassendes Team zur Kinder- und Jugendförderung. Diese leisten auch in den freiwilligen Angeboten der Stadt, wie z. B. den Jugendtreffs oder Jugendzentren, Betreuungsarbeit. Neben der reinen Beaufsichtigung werden auch Tätigkeiten zur Kinderförderung, Mädchenarbeit, Stadtteilarbeit sowie

Unterstützung beim Übergang von der Schule zum Beruf und Unterstützungsangebote zur Förderung von Schulen erbracht.

Im Rahmen dieser Tätigkeiten besteht nicht selten die Notwendigkeit, sich über einzelne Kinder und Jugendliche oder über Geschehnisse und Vorfälle innerhalb der Gruppen in den Jugendzentren auszutauschen. Dieser Austausch wird u. a. auch mit dem in § 8a SGB VIII geregelten Schutzauftrag bei Kindeswohlgefährdung begründet. Unter den Teammitgliedern besteht allerdings eine große Unsicherheit, inwieweit sie dabei die ihnen obliegende Schweigepflicht nach § 203 StGB zu beachten haben. Eine Stadt bat mich um Beratung, wie innerhalb des Teams ein zulässiger Austausch erfolgen kann.

Betreuer und Betreuerinnen unterliegen als Angehörige der Berufsgruppe „staatliche anerkannte Sozialarbeiter/Sozialpädagogen“ der Schweigepflicht nach § 203 Abs. 1 Nr. 5 StGB.

§ 203 Abs. 1 StGB

Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als …
5. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen … anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Mit dieser Vorschrift werden grundsätzlich der persönliche Lebens- und Geheimnisbereich des Betroffenen vor unbefugter Offenbarung und das Vertrauen in die Verschwiegenheit der verpflichteten Person geschützt. Dabei muss es sich allerdings um ein anvertrautes Geheimnis handeln, also um eine Tatsache, die nur einem Einzelnen oder einem beschränkten Personenkreis bekannt ist und an deren Geheimhaltung die/der Betroffene ein verständlich schutzwürdiges Interesse hat.

Die interne Besprechung allgemeiner Umstände und Geschehnisse innerhalb des Teams erfüllen bereits diese Tatbestandmerkmale nicht und unterfallen auch nicht der besonderen strafbewehrten Schweigepflicht, sondern sind unter den allgemeinen für das Berufsgeheimnis zu beachtenden Datenschutzgesichtspunkten zu behandeln.

Bei Zweifeln, ob nicht doch ein Geheimnis Gegenstand der Besprechung werden würde, ist zu beachten, dass eine Offenbarung nach § 203 StGB nur dann unbefugt ist, wenn keine Gründe vorliegen, die eine Offenbarung rechtfertigen. Solche rechtfertigenden Gründe bestehen, wenn die Voraussetzungen des § 8a Abs. 1 und 5 SGB VIII vorliegen. In diesen Fällen, in denen die Gefährdung des Kindeswohls zu beurteilen ist, können vertrauliche Daten, die zum persönlichen Lebensbereich eines Betroffenen gehören, trotz der strafbewehrten Schweigepflicht des § 203 StGB offenbart werden.

§ 8a Abs. 1 und 5 SGB VIII

(1) Werden dem Jugendamt gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so hat es das Gefährdungsrisiko im Zusammenwirken mehrerer Fachkräfte einzuschätzen. Soweit der wirksame Schutz dieses Kindes oder dieses Jugendlichen nicht in Frage gestellt wird, hat das Jugendamt die Erziehungsberechtigten sowie das Kind oder den Jugendlichen in die Gefährdungseinschätzung einzubeziehen und, sofern dies nach fachlicher Einschätzung erforderlich ist, sich dabei einen unmittelbaren Eindruck von dem Kind und von seiner persönlichen Umgebung zu verschaffen. Hält das Jugendamt zur Abwendung der Gefährdung die Gewährung von Hilfen für geeignet und notwendig, so hat es diese den Erziehungsberechtigten anzubieten.

(5) Werden einem örtlichen Träger gewichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder eines Jugendlichen bekannt, so sind dem für die Gewährung von Leistungen zuständigen örtlichen Träger die Daten mitzuteilen, deren Kenntnis zur Wahrnehmung des Schutzauftrags bei Kindeswohlgefährdung nach § 8a erforderlich ist. Die Mitteilung soll im Rahmen eines Gespräches zwischen den Fachkräften der beiden örtlichen Träger erfolgen, an dem die Personensorgeberechtigten sowie das Kind oder der Jugendliche beteiligt werden sollen, soweit hierdurch der wirksame Schutz des Kindes oder des Jugendlichen nicht in Frage gestellt wird.

Wenn sich Beschäftigte innerhalb des Teams über gewichtige Angelegenheiten in erforderlicher Art und Weise, objektivierbar und nachvollziehbar im Rahmen ihrer beruflichen Profession austauschen, um ein Gefährdungspotential zu erkennen und festzustellen, ob erforderliche Maßnahmen einzuleiten sind, so geschieht dies zur Aufgabenerfüllung ihrer beruflichen Tätigkeit. Die damit einhergehende Nutzung (interne Weitergabe) personenbezogener Daten ist dann zulässig, da es zur Erfüllung der Schutzaufgabe nach § 8a SGB VIII erforderlich ist, die Daten im Rahmen einer Teambesprechung oder Supervision intern auszutauschen.

Dies gilt auch für Daten, die nicht unmittelbar zur Erfüllung der Aufgaben „Sozialarbeiter/Sozialarbeiterin“ oder „Sozialpädagoge/Sozialpädagogin“ verwendet werden, sondern als „Annexe“ der Aufgabenerfüllung erforderlich sind, z. B. für Organisation, Kontrolle oder Planung.

Beim Umgang mit besonders anvertrauten Daten (vgl. § 65 SGB VIII) muss allerdings in jedem Einzelfall gesondert gewichtet und entschieden werden; hier muss ggf. die Einwilligung der/des Betroffenen eingeholt werden, um § 203 StGB nicht zu verletzen.

§ 65 Abs. 1 SGB VIII

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

1. mit der Einwilligung dessen, der die Daten anvertraut hat, oder

…

5. unter den Voraussetzungen, unter denen eine der in § 203 Abs. 1 oder 3 des Strafgesetzbuches genannten Personen dazu befugt wäre.

3.2.3

Gewährleistung des sog. „U3-Rechtsanspruchs“ zur Betreuung von Kindern im Alter unter drei Jahren mit Hilfe von unterstützender Software

Im Bereich der Kinder- und Jugendhilfe besteht in Hessen seit 01.08.2013 ein Rechtsanspruch auf einen Betreuungsplatz (sog. U3-Rechtsanspruch). Um diesen Anspruch effektiv, rechtskonform und wirtschaftlich sinnvoll umzusetzen, bedient sich die Mehrzahl der zuständigen Behörden der EDV und hier spezieller Software. Dabei kann es zu datenschutzrechtlichen Problemen kommen. Daher habe ich eine große hessische Stadt bei deren Projekt mit einem Softwareanbieter und der daraus entstehenden bzw. resultierenden Auftragsdatenverarbeitung hierzu über Monate (sozial-)datenschutzrechtlich beratend begleitet. In diesem Prozess kam es am Ende zu einer für alle Beteiligten akzeptablen Softwarelösung und wegen einer speziellen Besonderheit im Projektverlauf letztendlich zu einer Änderung der Kindertagesstättenverordnung der Evangelischen Kirche in Hessen und Nassau (EKHN), um den praktischen Erfordernissen in diesem Themenkomplex besser gerecht werden zu können.

Die behördliche Datenschutzbeauftragte und das eingesetzte Projektteam der Stadt haben sich sehr frühzeitig an mich gewandt und ihre ersten Arbeitsergebnisse zum geplanten Softwareeinsatz vorgelegt. Mit Hilfe einer modular aufgebauten Software solle die elektronische Abwicklung der Verwaltungsvorgänge im Bereich der Förderung und Betreuung der Kinder in Kindertageseinrichtungen und Kindertagespflege unterstützt werden – und zwar von der Anmeldung der Kinder in der Kita durch die Personensorgeberechtigten bis zur Planung eines bedarfsgerechten Angebots durch den örtlichen Träger der öffentlichen Jugendhilfe. Die Stadt beabsichtige, das Softwareverfahren extern "hosten" zu lassen. Dadurch werde eine Auftragsdatenverarbeitung ausgelöst.

Es zeigte sich schnell, dass die Stadt bereits gute Vorarbeit zu dieser rechtlich durchaus komplexen Materie geleistet hatte, aber auch, dass sie einen zugänglichen, gesprächsbereiten Softwareanbieter gewonnen hatte, der sich nicht zuletzt auch zu Fragen und Anforderungen des Datenschutzes zu seinem bzw. an sein Produkt kooperativ zeigte. Dies wurde in einem gemeinsamen Termin, in dem die Software mit ihren Funktionalitäten von diesem präsentiert wurde, bestätigt. Hier zeigte sich auch „live“, dass zum einen das vorhandene und hier vorgelegte Datenschutz- und Sicherheitskonzept gut eingebettet und funktional war. Zum anderen wurde deutlich, dass die Nutzungsoptionen die Stadt mannigfaltig unterstützen und ihr helfen, ihren gesetzlichen Aufgaben besser nachzukommen.

Als problematisch in diesem Projekt kristallisierte sich dagegen eine Positionierung des Datenschutzbeauftragten der EKHN heraus, deren Kindertageseinrichtungen ebenfalls an der Software „andocken“ und partizipieren sollten. Danach gebe es für die EKHN im kirchlichen Datenschutzrecht keine Übermittlungsbefugnis, die es erlaubte, Daten von dort in die Software der Stadt zu übertragen. Eine solche Befugnis benötige sie aber z. B. in den Fällen, in denen Eltern direkt in den kirchlichen Kindergarten kämen und ihr Kind dort anmelden wollten. In diesen Fällen sei der Kindergarten die „erste“ datenverarbeitende Stelle und benötige eine Rechtsgrundlage, um diese Daten in die Software bzw. an den Jugendhilfeträger übermitteln zu können. Das SGB gelte für den Bereich der Kirche nicht, darauf könne sich das Jugendamt bzw. der Träger der öffentlichen Jugendhilfe berufen, nicht jedoch die Kirche. Man brauche entweder eine Rechtsvorschrift, die dies gestatte, die gebe es jedoch nicht, oder die Übermittlung müsse „im kirchlichen Auftrag“ erfolgen bzw. mit diesem in Zusammenhang stehen, was vorliegend nicht ohne Weiteres anzunehmen sei und unterstellt werden könne.

Durch diese Auffassung wurde das Projekt lange Zeit blockiert. Die Auffassung ist jedoch rechtlich aus folgenden Gründen nicht haltbar: Die Kirchen und Religionsgemeinschaften des öffentlichen Rechts sowie die auf Bundesebene zusammengeschlossenen Verbände der freien Wohlfahrtspflege sind anerkannte Träger der freien Jugendhilfe gemäß § 75 Abs. 3 SGB VIII.

§ 75 Abs. 3 SGB VIII

Die Kirchen und Religionsgemeinschaften des öffentlichen Rechts sowie die auf Bundesebene zusammengeschlossenen Verbände der freien Wohlfahrtspflege sind anerkannte Träger der freien Jugendhilfe.

Werden Einrichtungen und Dienste der Träger der freien Jugendhilfe in Anspruch genommen, so ist sicherzustellen, dass der Schutz der personenbezogenen Daten bei der Erhebung und Verwendung in entsprechender Weise gewährleistet ist, § 61 Abs. 3 SGB VIII. „In entsprechender Weise“ meint, so wie es in § 61 Abs. 1 SGB VIII beschrieben ist.

§ 61 Abs. 1 und 3 SGB VIII

(1) Für den Schutz von Sozialdaten bei ihrer Erhebung und Verwendung in der Jugendhilfe gelten § 35 des Ersten Buches, §§ 67 bis 85a des Zehnten Buches sowie die nachfolgenden Vorschriften. Sie gelten für alle Stellen des Trägers der öffentlichen Jugendhilfe, soweit sie Aufgaben nach diesem Buch wahrnehmen. Für die Wahrnehmung von Aufgaben nach diesem Buch durch kreisangehörige Gemeinden und Gemeindeverbände, die nicht örtliche Träger sind, gelten die Sätze 1 und 2 entsprechend.

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

Für Kirchen, die nicht Leistungsträger im Sinne von § 35 SGB I sind, gelten grundsätzlich nur deren trägerinterner Sozialdatenschutz sowie die allgemeinen Regelungen des BDSG bzw. des jeweiligen Landesdatenschutzrechtes.

Aber: Vollkommen unstrittig findet das Sozialdatenschutzrecht des SGB mittelbar über die Sicherstellungsverpflichtung der freien Träger gemäß § 61 Abs. 3 SGB VIII Anwendung. Dies führt zu einer faktischen Gleichbehandlung des Sozialdatenschutzes bei freien und

öffentlichen Trägern [Proksch in Münder/Meysen/Trenczek, Frankfurter Kommentar SGB VIII, 6. Aufl. 2009, Vorbemerkung zum 4. Kapitel (§§ 61-68), Rdnr. 28]. § 61 Abs. 3 SGB VIII regelt also die Verlängerung der Datenschutzverpflichtungen im Fall der Inanspruchnahme von Einrichtungen und Diensten der Träger der freien Jugendhilfe. Für diese darf nichts anderes gelten als für diejenigen der Träger der öffentlichen Jugendhilfe. Der Schutz gilt für alle personenbezogenen Daten, die der freie Träger selbst einholt und die auch das Jugendamt zu schützen hätte. Der Schutz gilt aber auch gegenüber dem Jugendamt selbst. Der Träger der öffentlichen Jugendhilfe ist also Garant dafür, dass der Datenschutz bei den freien Trägern entsprechend den Vorgaben im SGB VIII beachtet wird. Dies gilt sowohl für die zu beachtenden Beschränkungen wie auch für Eingriffsbefugnisse. Datenschutz im Sinne dieser Normen heißt auch, dass den Einrichtungen und Diensten der Träger der freien Jugendhilfe nur die zur Wahrnehmung ihrer jeweiligen Aufgabe erforderlichen Daten zugänglich gemacht werden und umgekehrt, **dass der öffentliche Träger der Jugendhilfe vom freien Träger nur die Informationen verlangen kann, die für seine Aufgabenerfüllung erforderlich sind** (Proksch in Münder/Meysen/Trenczek, Frankfurter Kommentar SGB VIII, 6. Aufl. 2009, zu § 61, Rdnr. 23).

Nachdem die Stadt sich dann im weiteren Verlauf mit dem Softwareanbieter und auch einzelnen Auftragnehmern von diesem auf Vertragswerke verständigt hatte, die sowohl den rechtlichen, insbesondere sozialdatenschutzrechtlichen, als auch den technischen Vorgaben gerecht wurden, konnte das Projekt von dieser schließlich erfolgreich abgeschlossen werden. Das Angebot wurde dann der Öffentlichkeit präsentiert und „live“ geschaltet und erfreut sich guter Akzeptanz.

Mit einigem zeitlichem Nachgang habe ich dann erfahren, dass es eine Neuerung in der Kindertagesstättenverordnung der EKHN gegeben hatte. Offenbar war die eben skizzierte Auseinandersetzung hierfür mit der Auslöser. In dieser Verordnung regelt ein Paragraph, § 3, Träger und Trägerschaft von Kindertagesstätten. Dieser § 3 wurde um einen Absatz 9 ergänzt.

§ 3 Abs. 9 Kindertagesstättenverordnung (der EKHN)

Die Träger können auf Verlangen der Kommunen im Rahmen elektronischer Anmeldeverfahren für Kindertagesstätten diesen Auskünfte über die Namen, die Anschriften und die Geburtsdaten der angemeldeten Kinder und Namen, Adresse und Telefonnummer eines Erziehungsberechtigten sowie den gewünschten Aufnahmetermin, Betreuungsumfang und Betreuungszeit übermitteln. Kommt es zum Abschluss eines Betreuungsvertrages in

einer Kindertagesstätte, sind darüber hinaus das Datum des Vertragsbeginns und das Enddatum, der Betreuungsumfang, die Betreuungszeiten, der voraussichtliche Einschulungstermin und Daten zur Vertragsänderung mitzuteilen. In allen anderen Fällen ist die Übermittlung von Namen und Geburtsdaten sowie Betreuungsart und -umfang zulässig. Die Daten dürfen elektronisch übermittelt werden, wenn die Vertraulichkeit durch geeignete technische Maßnahmen sichergestellt ist.

3.2.4
Aufsichtsbehörde bei einer Auftragsdatenverarbeitung im Sozialwesen nach § 80 SGB X

Bei einer Auftragsdatenverarbeitung im Sozialwesen ist Adressat der schriftlichen Anzeige nach § 80 SGB X die Fachaufsichtsbehörde und nicht die Datenschutzaufsichtsbehörde.

Eine Stadt war sich bei der Umsetzung der rechtlichen Vorgaben bei der Auftragsdatenverarbeitung im Sozialwesen unsicher, welche Stelle mit Aufsichtsbehörde im Sinne des § 80 SGB X gemeint ist. Die Unsicherheit resultierte auch aus der Reaktion der zuständigen Aufsichtsbehörde, die sich für unzuständig erklärte und an mich verwies. Das Jugendamt der Stadt wollte eine Software neu einführen und sich hierfür eines Dritten bedienen, der für die Stadt nach Abschluss eines Vertrages hierüber tätig werden sollte. Dies ist grundsätzlich auch im Sozialwesen möglich und geht aus § 80 SGB X hervor.

§ 80 Abs. 1 und 2 SGB X

(1) Werden Sozialdaten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzbuches und anderer Vorschriften über den Datenschutz verantwortlich. ...

(2) Eine Auftragserteilung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten ist nur zulässig, wenn der Datenschutz beim Auftragnehmer nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten den Anforderungen genügt, die für den Auftraggeber gelten. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind: …

Die Umsetzung der sich insbesondere aus Absatz 2 ergebenden Vorgaben beinhaltet die rechtzeitige Mitteilung vor der Auftragserteilung vom Auftraggeber, also dem

Sozialleistungsträger bzw. der Stadt, an die Aufsichtsbehörde. Dies gibt § 80 Abs. 3 SGB X so vor.

§ 80 Abs. 3 SGB X

Der Auftraggeber hat seiner Aufsichtsbehörde rechtzeitig vor der Auftragserteilung
1. den Auftragnehmer, die bei diesem vorhandenen technischen und organisatorischen Maßnahmen und ergänzenden Weisungen nach Absatz 2 Satz 2 und 3,
2. die Art der Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden sollen, und den Kreis der Betroffenen,
3. die Aufgabe, zu deren Erfüllung die Erhebung, Verarbeitung oder Nutzung der Daten im Auftrag erfolgen soll, sowie
4. den Abschluss von etwaigen Unterauftragsverhältnissen

schriftlich anzuzeigen. …

Das Jugendamt der Stadt hatte nun versucht, dieser Pflicht gegenüber dem für sich zuständigen Regierungspräsidium bzw. diesem übergeordnet dem Hessischen Sozialministerium nachzukommen. Beide Stellen hätten sich aber gegenüber der Stadt dahingehend geäußert, sie seien nicht als „Aufsichtsbehörde“ von und nach § 80 SGB X angesprochen.

Diese Stellungnahmen nahm die Stadt zum Anlass, mich zu fragen, ob ich mich bezüglich § 80 Abs. 3 SGB X als Aufsichtsbehörde fühle.

Bereits aus der Gesetzessystematik des § 80 SGB X ergibt sich aus meiner Sicht, wer bei der vorliegenden Fallkonstellation als „Aufsichtsbehörde“ angesprochen ist.

Denn in § 80 Abs. 6 SGB X wird ausdrücklich normiert, wie bzw. durch welche Stelle die Datenschutzaufsicht wahrgenommen wird/werden muss, entweder durch die/den Bundesbeauftragte/-n für den Datenschutz und die Informationsfreiheit oder durch die/den Landesbeauftragte/-n für den Datenschutz, deren/dessen Aufgaben und Befugnisse sich nach dem jeweiligen Landesrecht richten.

§ 80 Abs. 6 SGB X

Ist der Auftragnehmer eine in § 35 des Ersten Buches genannte Stelle, gelten neben den §§ 85 und 85a nur § 4g Abs. 2, § 18 Abs. 2 und die §§ 24 bis 26 des

Bundesdatenschutzgesetzes. Bei den in § 35 des Ersten Buches genannten Stellen, die nicht solche des Bundes sind, treten anstelle des Bundesbeauftragten für den Datenschutz insoweit die Landesbeauftragten für den Datenschutz. Ihre Aufgaben und Befugnisse richten sich nach dem jeweiligen Landesrecht. Ist der Auftragnehmer eine nicht-öffentliche Stelle, kontrolliert die Einhaltung der Absätze 1 bis 5 die nach Landesrecht zuständige Aufsichtsbehörde. Bei öffentlichen Stellen der Länder, die nicht Sozialversicherungsträger oder deren Verbände sind, gelten die landesrechtlichen Vorschriften über Verzeichnisse der eingesetzten Datenverarbeitungsanlagen und Dateien.

Abs. 6 vorgehend wird in § 80 Abs. 3 SGB X, zugegeben recht „allgemein", von „Aufsichtsbehörde" gesprochen (s. o.). Hierbei muss es sich dann, vgl. Abs. 6, um eine andere Stelle/Behörde handeln. Dies ist die Fachaufsichtsbehörde.

In der Kommentierung zum § 80 Abs. 3 SGB X von Rombach in Hauck/Noftz, SGB X K § 80, Rdnr. 69, wird beispielhaft aufgeführt, dass „bei bundesunmittelbaren Sozialversicherungsträgern (…) die Aufgaben der Aufsichtsbehörde das Bundesverwaltungsamt in Berlin wahr[nimmt] (§ 90 Abs. 1 SGB IV), bei landesunmittelbaren Sozialversicherungsträgern die Stellen nach § 90 Abs. 2 SGB IV, im Falle der Einigung beteiligter Länder (maximal drei) auf ein Aufsicht führendes Land nimmt die zuständige Landesbehörde auch bei Sozialversicherungsträgern, die sich maximal auf drei Länder erstrecken, die Aufsicht wahr (§ 90 Abs. 3 SGB IV, teilweise sind die Versicherungsämter der Länder Aufsichtsbehörden [vgl. §§ 92 f. SGB IV; Fattler in Hauck/Noftz, SGB IV K § 93, Rdnr. 5])." Auch hieraus lässt sich schließen und entnehmen, dass § 80 Abs. 3 SGB X Fachaufsichtsbehörden im Fokus hat.

Für die hier vorgelegte Fallkonstellation im Bereich der Kinder- und Jugendhilfe gibt es zudem hessische Ausführungsvorschriften zur Umsetzung des SGB VIII im Land Hessen, das Hessische Kinder- und Jugendhilfegesetzbuch (HKJGB). Diese regeln die Aufsicht in § 7a Abs. 1 HKJGB:

§ 7a Abs. 1 HKJGB

Die örtlichen Träger der öffentlichen Jugendhilfe unterliegen der Rechtsaufsicht des Staates. Zuständige Aufsichtsbehörde ist das Regierungspräsidium. Obere Aufsichtsbehörde ist das für die Jugendhilfe zuständige Ministerium.

Dies habe ich der Stadt entsprechend mitgeteilt, welche die Information mit meinem Einverständnis direkt auch an die beiden zuständigen Aufsichtsbehörden weitergeben wollte.

3.3
Landkreise und Kommunen

3.3.1
Praxis der Bearbeitung von OWi-Verfahren – insbesondere von Verkehrsverstößen – in Kommunen

Trotz regelmäßiger Beschwerden über die Bearbeitung von Verkehrsordnungswidrigkeiten konnten bei einer stichprobenartigen Überprüfung keine Datenschutzverletzungen festgestellt werden. Auch der Einsatz von Handys zur Datenerfassung ist grundsätzlich möglich.

Immer wieder habe ich verschiedenste Anfragen zur Behandlung von Verkehrsordnungswidrigkeiten durch die Ordnungsbehörden. Die Verfolgung und Ahndung von Verkehrsordnungswidrigkeiten wird durch Polizeibehörden und allgemeine Ordnungsbehörden wahrgenommen und dient der Sicherheit des Straßenverkehrs. Im Berichtsjahr überprüfte ich die Praxis der Bearbeitung von Verkehrsverstößen im fließenden und ruhenden Verkehr in sieben hessischen Kommunen.

In allen überprüften Kommunen hatten die für die Verkehrsüberwachung und Verfolgung der Verkehrsordnungswidrigkeiten zuständigen Mitarbeiterinnen und Mitarbeiter die entsprechenden Schulungen bei der Polizeiakademie Hessen absolviert. Ebenso lagen immer die erforderlichen Bestellungsverfügungen der jeweiligen Landkreise vor.

3.3.1.1
Überwachung des fließenden Verkehrs

Bei den überprüften Kommunen wurden zwischen 20.000 und 72.000 Ordnungswidrigkeiten im Jahr 2014 festgestellt und bearbeitet. Die Zahl der hierbei eingesetzten stationären Geräte reichte von 2 bis 24 stationären Blitzanlagen. Diese wurden in den meisten Kommunen durch angemietete mobile Blitzgeräte ergänzt. Nicht alle stationären Blitzanlagen waren auch tatsächlich betriebsbereit.

Das regelmäßige Auslesen der in den Blitzanlagen gespeicherten Bilder von Verkehrsordnungswidrigkeiten erfolgte entweder durch Mitarbeiterinnen und Mitarbeiter der Ordnungswidrigkeitenbehörden selbst oder es wurden externe Dienstleister mit dieser Aufgabe betraut. Die Daten werden vor Ort mit Laptop, USB-Stick oder mittels Datenfernabfrage ausgelesen. Die daran anschließende Aufbereitung der Rohdaten zur Überleitung in die eingesetzten Verfahren erfolgte entweder eigenständig durch die Mitarbeiterinnen und Mitarbeiter der Kommunen oder durch Dienstleister. Hierbei konnte in jedem Fall ein Dienstleistungsvertrag für diese Auftragsdatenverarbeitung vorgelegt werden.

Von allen Ordnungsbehörden wurde berücksichtigt, dass die Verfolgung von Ordnungswidrigkeiten eine hoheitliche Aufgabe ist und deshalb nicht delegiert werden kann. Alle aufbereiteten Daten wurden vor dem Einstellen in das jeweils genutzte Verfahren durch geschulte Mitarbeiterinnen oder Mitarbeiter der Ordnungsbehörden gesichtet und die weitere Verwendung im Einzelfall entschieden. Hierbei wird anhand der Qualität und des Inhalts der Bilder abgewogen, ob sich die Lichtbilder zur Identifizierung der Fahrzeugführerin oder des Fahrzeugführers eignen. Nach dieser Entscheidung über die Verfolgung einer Ordnungswidrigkeit werden die durch die Blitzanlagen ermittelten Daten in das hierfür genutzte Programm hochgeladen. Überwiegend wird von hessischen Kommunen das Programm OWi21 genutzt, es sind aber auch Programme anderer Anbieter bei Kommunen im Einsatz.

Nach einer automatisierten Abfrage der Halterdaten der geblitzten Fahrzeuge beim Kraftfahrt-Bundesamt erfolgt bei geringfügigeren Verstößen ein Angebot zur Zahlung eines Verwarngeldes, dies wird von der für die Überwachungsanlage zuständigen Ordnungsbehörde selbst durchgeführt. Bei schwereren Verstößen gegen die Straßenverkehrsordnung erfolgt die Verfolgung und Ahndung durch die hessische zentrale Bußgeldstelle beim Regierungspräsidium Kassel.

Ist anhand des vorhandenen Bildmaterials eindeutig erkennbar, dass Fahrzeughalter und geblitzter Fahrer (Geschlecht, Alter) nicht übereinstimmen oder ist der Fahrzeughalter eine Firma, so wird statt des Verwarngeld-Angebots ein Zeugenfragebogen verschickt.

Nur in einer Kommune enthielten die Verwarngeld-Angebote und Zeugenfragebogen keinen Hinweis auf einen möglichen Lichtbildabgleich mit der Passdatei. Ferner wurde in allen Anschreiben auf ein Zeugnisverweigerungsrecht hingewiesen. Mir wurde zugesagt, den fehlenden Hinweis auf einen möglichen Lichtbildabgleich in die Anschreiben aufzunehmen,

da ein Lichtbildabgleich nur zulässig ist, wenn der Betroffene vorher auf diese Möglichkeit hingewiesen wurde.

Reagiert der angeschriebene Fahrzeughalter nicht auf das Verwarngeld-Angebot oder den Zeugenfragebogen bzw. ergibt sich kein entsprechender Ermittlungserfolg hieraus, so führen die Ordnungsbehörden zunächst alle ihnen möglichen Ermittlungen durch. Hierzu gehören Abfragen im Einwohnermelderegister und Einsichtnahmen in Pass- und Personalausweisregister. Ein förmliches Ersuchen wird an den Wohnort des Fahrzeughalters gerichtet oder wenn es sich um den eigenen Ort handelt selbst ermittelt. Dabei konnte ich in einer Kommune feststellen, dass die Ordnungswidrigkeitenbehörde einen eigenen Zugriff auf die Personalausweisdatei hatte. In einer anderen Kommune war die Leiterin der Ordnungsbehörde auch Leiterin der Meldebehörde. Das Ersuchen auf Übersendung einer Kopie des Lichtbildes aus der Personalausweis- oder Passdatei ist nach § 24 Abs. 3 PAuswG bzw. § 22 PaßG zulässig, wenn zunächst versucht wurde, die Daten beim Betroffenen selbst zu erheben. Dabei muss sich das Ersuchen auf eine konkrete Person beziehen. Über diese Phase der Verfolgung von Ordnungswidrigkeiten liegen mir häufiger Datenschutzbeschwerden vor. Bei meinen Prüfungen konnte ich aber keine Anhaltspunkte dafür feststellen, dass der Lichtbildabgleich nicht korrekt umgesetzt wird.

Generell wurde mir von allen überprüften Ordnungsbehörden versichert, dass von dem Lichtbildvergleich nur in geringem Umfang Gebrauch gemacht werden muss. Ebenso beschränken sich Ermittlungen vor Ort auf wenige Ordnungswidrigkeitenverfahren. Dies gilt auch für die Einschaltung eines Anwalts durch den Fahrzeughalter. Auch hier konnte ich keinen Einfluss auf den Ablauf des Verfahrens feststellen. Anwälte bekamen regelmäßig die von ihnen angeforderten Unterlagen.

Im Bereich der Verfolgung von Verkehrsverstößen konnte ich bei meiner stichprobenhaften Überprüfung keine datenschutzrechtlichen Mängel feststellen. Die Übertragung von Aufgaben an private Dritte erfolgte nur in dem zulässigen Umfang und schloss hoheitliche Aufgaben und Entscheidungen immer aus. Die Verhältnismäßigkeit der getroffenen Ermittlungsmaßnahmen wurde in allen Fällen gewahrt.

3.3.1.2
Überwachung des ruhenden Straßenverkehrs

3.3.1.2.1
Einsatz von Smartphones zur Datenerfassung

Die Feststellung von Verkehrsordnungswidrigkeiten im ruhenden Verkehr erfolgt auf den Straßen durch Mitarbeiterinnen und Mitarbeiter des Ordnungsamtes. Hierfür standen zum Teil Smartphones zur Verfügung, die über eine zu den jeweils eingesetzten Ordnungswidrigkeitenverfahren entwickelte App verfügen und von der Kommune für dienstliche Zwecke zur Verfügung gestellt werden. Neben der Erfassung des Kennzeichens werden auch entsprechende Beweisfotos erstellt. Hierbei ist sichergestellt, dass alle anderen Anwendungen eines Smartphones auf diese Bilddateien nicht zugreifen können. Zur Nutzung dieser App waren immer eine Benutzerkennung und ein Passwort nötig, um eine unberechtigte Nutzung auszuschließen. Die Übernahme der erfassten Ordnungswidrigkeiten in die für die Bearbeitung aller Ordnungswidrigkeiten genutzten Programme erfolgte verschlüsselt über das Internet, aber auch mit Hilfe eines Netzwerkkabels in der jeweiligen Dienststelle. Die weitere Bearbeitung entspricht den Regeln für Ordnungswidrigkeiten im fließenden Verkehr.

3.3.1.2.2
Anforderungen an die Nutzung des Smartphones

Die von der App zu einer Ordnungswidrigkeit verarbeiteten Daten werden auf dem Smartphone verschlüsselt gespeichert. Nach einer erfolgreichen Übertragung werden die Daten umgehend gelöscht. Dank dieser Abläufe ist die Gefahr einer unberechtigten Kenntnisnahme verringert. Schon im 42. Tätigkeitsbericht (Ziff. 3.3.2.4.2) hatte ich im Zusammenhang mit der Nutzung von Smartphones durch die Polizei die notwendigen Datensicherheitsanforderungen dargelegt.

Diese Anforderungen gelten selbstverständlich auch für die Gefahrenabwehrbehörden. In einer „**Handreichung zur Nutzung von Smartphones und Tablet-Computer in Behörden und Unternehmen“** (Homepage HDSB: Fachthemen/Mobile Geräte/Handreichung zu Nutzung von Smartphones ...) habe ich Anforderungen detailliert aufgeführt. Wesentliche Punkte möchte ich an dieser Stelle noch einmal benennen:

– Da Daten zu Ordnungswidrigkeiten, also hoheitliche Daten, verarbeitet werden, halte ich es für zwingend, dass das Smartphone ein Dienstgerät ist.

– Der Umgang mit dem Dienstgerät sollte durch eine Dienstanweisung geregelt werden. Eine private Nutzung sollte untersagt werden. Ggfs. kann bei Telefonaten eine Ausnahme gemacht werden. Dann müssen aber die Rahmenbedingungen in einer Dienstvereinbarung festgelegt sein.

– Es ist ein MDM (Mobile Device Management) zur Verwaltung der Geräteeinstellungen einzusetzen. Damit sind die Grundeinstellungen für die Datensicherheit so zu setzen, dass sie zumindest nicht schwächer sind als bei der stationären IT.
Auch sollten nicht benötigte Schnittstellen sowohl durch Geräteeinstellungen als auch im MDM-System gesperrt werden, die Installation von nicht zugelassenen Apps unterbunden werden und die Möglichkeit vorgesehen sein, beispielsweise bei Verlust des Smartphones, die Daten aus der Ferne zu löschen.

– Sollte das Smartphone gerootet sein, also eine Manipulation am Betriebssystem stattgefunden haben, muss ebenfalls eine Reaktion des MDM erfolgen; hier halte ich eine Fernlöschung für angebracht.

Wenn die entsprechenden Maßnahmen umgesetzt sind, ergeben sich auch aus der Nutzung von Smartphones keine Probleme.

3.3.2
Nutzung des E-Post-Briefes

Viele öffentliche Stellen, vor allem Kommunen, wollen für ihren Massenbriefversand aus Kostengründen den E-Post-Brief der Deutschen Post AG nutzen. Schriftstücke, deren Inhalt einer besonderen Geheimhaltung unterliegt, sind allerdings für die Versandform Hybridbrief nicht geeignet.

Die Deutsche Post AG bietet den E-Post-Brief derzeit in den Versandvarianten Hybridbrief und vollelektronischer Versand an.

3.3.2.1
Hybridbrief

Beim Hybridbrief ist nur der Absender des E-Post-Briefs registrierter Kunde des E-Post-Brief-Verfahrens. Der vom Absender elektronisch erstellte Brief wird durch die Deutsche Post AG ausgedruckt, kuvertiert und dem Empfänger auf dem normalen Postweg als Briefpost zugestellt. Diese Dienstleistung der Post ist rechtlich als Datenverarbeitung im Auftrag gemäß § 4 HDSG zu werten. Die Kommune oder eine andere öffentliche Stelle als Auftraggeber ist deshalb verpflichtet, vertraglich sicherzustellen, dass die Post AG die Vorschriften des HDSG befolgt und sich der Kontrolle durch den Hessischen Datenschutzbeauftragten unterwirft.

3.3.2.2
Vollelektronischer Versand

Beim vollelektronischen Versand sind beide Teilnehmer am Verfahren registrierte Kunden des E-Post-Brief-Verfahrens. Der Brief wird hier vom Absender direkt an den Empfänger elektronisch versandt. Die Post wird hier nicht als Auftragnehmer im unter Ziff. 3.3.2.1 beschriebenen Sinne tätig.

Der vollelektronische Versand wird in zwei unterschiedlichen Modellen angeboten. Bei der ursprünglichen Variante werden die Daten unverschlüsselt an den Empfänger übertragen. Seit dem Jahr 2013 bietet die Deutsche Post AG Großkunden bei Nutzung des vollelektronischen Versands an, die Anhänge in einer Ende-zu-Ende-verschlüsselten Form zu übersenden. Die Anhänge werden dabei vom Absender mit Hilfe des Empfängerzertifikats verschlüsselt und einem normalen E-Post-Brief als Anhang beigefügt.

Immer wieder wurde die Frage gestellt, ob der E-Post-Brief genutzt werden kann, wenn Daten versandt werden sollen, die einem besonderen Berufs- oder Amtsgeheimnis bzw. einem erhöhten Schutzbedarf unterliegen. Ich habe gegenüber den anfragenden Stellen hervorgehoben, dass die Varianten Hybridbrief und unverschlüsselter vollelektronischer Versand für Daten mit erhöhtem Schutzbedarf (Sozial-, Gesundheits- und Steuerdaten) aus Datenschutz- und Datensicherheitsgründen nicht in Betracht kommen, die zuletzt beschriebene Anhangverschlüsselung aber eine Lösung sein kann. Der Absender muss hier per Gateway am System der Deutschen Post AG angebunden sein. Der Absender bereitet die Anhänge bei sich vor, verschlüsselt sie nach den Vorgaben der Deutschen Post AG und mit Hilfe der durch den Verzeichnisdienst zur Verfügung gestellten Zertifikate. Im Zertifikat ist der öffentliche Schlüssel des jeweiligen Empfängers enthalten, der zur Verschlüsselung nötig

ist. Das stellt sicher, dass auch im Falle einer Falschzustellung der falsche Empfänger den Anhang nicht lesen kann, da die Schlüssel unterschiedlich sind.

Für Daten, die einem niedrigen Schutzbedarf unterliegen, kann der Hybridbrief unter den unter Ziff. 3.3.2.1 genannten Voraussetzungen eingesetzt werden. Das „normale“ vollelektronische Versandverfahren kann für den Versand von Daten mit niedrigem Schutzbedarf dann eingesetzt werden, wenn der Bürger gegenüber der Verwaltung diesen Versandweg autorisiert hat.

Seitens der Post AG ist geplant, zukünftig allen Kunden eine Verschlüsselungsoption verfügbar zu machen, wie sie jetzt für Geschäftskunden bereits existiert.

3.3.3
Arbeit von ehrenamtlichen Helfern mit Flüchtlingen

Der Beitrag stellt einige datenschutzrechtlich relevante Fragestellungen zusammen, die sich bei der Arbeit von ehrenamtlichen Helfern mit Flüchtlingen ergeben.

Im Berichtszeitraum – insbesondere im letzten halben Jahr – war zu beobachten, dass sich viele Bürgerinnen und Bürger ehrenamtlich für Flüchtlinge einsetzen. Dies kann zum Beispiel dadurch erfolgen, dass sie Begleitung bei Behördengängen anbieten, Fahrdienste übernehmen, sie bei der Eröffnung eines Bankkontos unterstützen, Sprachunterricht erteilen oder sie zur Teilnahme an Sportereignissen oder anderen sozialen Aktivitäten einladen.

In den letzten Monaten habe ich eine Reihe von Eingaben von Bürgern sowie Anfragen von Landkreisen und Kommunen erhalten, in denen es um Fragen zur Gewährleistung des Datenschutzes im Zusammenhang mit dem Engagement von ehrenamtlichen Helfern geht. Folgende Fragestellungen erscheinen mir wichtig:

3.3.3.1
Erfassung und Weitergabe personenbezogener Daten von ehrenamtlichen Helfern

Die Selbstorganisation der ehrenamtlichen Helfer ist unterschiedlich: Sie geht vom eingetragenen Verein, über den nicht rechtsfähigen Verein, über lose Zusammenschlüsse in

sog. Asylkreisen bis zur Übernahme von „Patenschaften“ durch einzelne Bürger für Flüchtlinge. Auch die Art der organisatorischen Anbindung an die Kommunen oder das zuständige Amt des Landkreises variiert.

Unabhängig von der Selbstorganisation haben die ehrenamtlichen Helfer ein Interesse daran, dass Daten wie Name, Telefonnummern, aber auch beispielsweise Angaben über bestimmte Kompetenzen (u. a. Fremdsprachen, Berufsqualifikation) erfasst und anderen Helfern zur Verfügung gestellt werden können.

Die Erstellung einer derartigen Liste auf elektronischem Weg beispielsweise durch den Vereinsvorstand oder Teilnehmer eines Asylkreises ist datenschutzrechtlich als eine Erhebung und Übermittlung von personenbezogenen Daten zu bewerten. Auch wenn der Verein oder Asylkreis von der zuständigen Behörde auf Kreisebene bzw. der Kommune organisatorisch oder finanziell unterstützt wird oder sogar im Einzelfall Personenidentität vorliegt, geht es um eine Datenverarbeitung durch Private. Mangels Weisungsbefugnis der öffentlichen Hand liegt keine Verwaltungshilfe vor, sondern nur eine rein private Betätigung. Anwendung findet deshalb das BDSG.

§ 1 Abs. 2 Nr. 3 BDSG

Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

...

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Die Voraussetzungen für eine rechtmäßige Datenverarbeitung sind in § 4 BDSG geregelt.

§ 4 Abs. 1 BDSG

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

Für Vereine, die nach ihrer Satzung bestimmte Ziele verfolgen- in den vorliegenden Fällen die Hilfe und Unterstützung von Flüchtlingen-, kommt als Rechtsgrundlage i. S. v. § 4 Abs. 1 für die Erstellung einer Mitgliederliste § 28 Abs. 1 Nr. 1 BDSG in Betracht.

§ 28 Abs. 1 Nr. 1 BDSG

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

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

...

Erhoben werden dürfen danach nur solche Daten, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande gekommenen rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Damit dürfen alle Daten erhoben werden, die zur Verfolgung der Vereinsziele und für die Betreuung und Verwaltung der Mitglieder benötigt werden.

Eine wie in § 4 Abs. 1 geforderte Rechtsvorschrift stellt die Vereinssatzung mangels ausreichender Rechtsqualität nicht dar.
Die Daten sind nach § 4 Abs. 2 S. 1 BDSG beim Betroffenen selbst zu erheben.

Bei loseren Zusammenschlüssen wie beispielsweise in Asylkreisen ist als Zulässigkeitsvoraussetzung i. S. v. § 4 Abs. 1 für die Datenerhebung und -übermittlung die Einwilligung des Betroffenen einzuholen. Dabei sind auch die Voraussetzungen von § 4a BDSG zu beachten.

§ 4a Abs. 1 BDSG

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

Je nach Einsatz der ehrenamtlichen Helfer kann von ihnen die Vorlage eines erweiterten Führungszeugnisses nach § 30a Bundeszentralregistergesetz (BZRG) verlangt werden.

§ 30a Abs. 1 Nr. 2 BZRG

Einer Person wird auf Antrag ein erweitertes Führungszeugnis erteilt,
...
2. wenn dieses Führungszeugnis benötigt wird für
   a) ...
   b) eine sonstige berufliche oder ehrenamtliche Beaufsichtigung, Betreuung, Erziehung oder Ausbildung Minderjähriger oder
   c) eine Tätigkeit, die in einer Buchstabe b vergleichbaren Weise geeignet ist, Kontakt zu Minderjährigen aufzunehmen.

Das Besondere an dem erweiterten Führungszeugnis ist, dass beispielsweise bestimmte Ausnahmen, die für Eintragungen im Zentralregister vorgesehen sind, nicht für Straftaten gegen die sexuelle Selbstbestimmung gelten. Die Einholung des erweiterten Führungszeugnisses kommt beispielsweise in Betracht, wenn die Helfer in die Betreuung Minderjähriger, insbesondere auch von unbegleiteten Minderjährigen eingebunden werden.

Das Führungszeugnis wird von der betroffenen Person beantragt und darf auch nur an den Antragsteller übersandt werden (§ 30a Abs. 2 i. V. m. § 30 Abs. 4 BZRG).

3.3.3.2
Erfassung und Weitergabe personenbezogener Daten von Flüchtlingen

Um ihre Arbeit mit Flüchtlingen effizient zu gestalten, müssen die ehrenamtlichen Helfer bestimmte personenbezogene Daten über die Flüchtlinge erhalten. Soweit diese Daten elektronisch verarbeitet werden, findet das BDSG Anwendung. Dies ist beispielsweise der Fall, wenn ein Verein oder Asylkreis eine elektronisch geführte Liste mit den Namen, Geburtsdaten und Aufenthaltsorten der von ihnen betreuten Flüchtlinge erstellt. Nach § 4 Abs. 1 BDSG bedarf es hierfür als Zulässigkeitsvoraussetzung der Einwilligung des Flüchtlings (§ 4a BDSG) und die Daten sind bei ihm selbst und nicht bei einem Dritten zu

erheben (§ 4 Abs. 2 BDSG). Die ehrenamtlichen Helfer sind des Weiteren auf das Datengeheimnis zu verpflichten (§ 5 BDSG).

§ 5 BDSG

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Daten, die sich auf den Rechnern der ehrenamtlichen Helfer befinden, müssen nach deren Ausscheiden gelöscht werden.

Begleitet die ehrenamtliche Helferin oder der ehrenamtliche Helfer den Flüchtling bei Behördengängen, beispielsweise dem Sozialamt, ist eine Offenbarung bestimmter durch das Sozialgeheimnis besonders geschützter Daten des Flüchtlings gegenüber dem Helfer oder der Helferin zunächst unzulässig (§ 35 Abs. 1 bis 3 SGB I und § 67 Abs. 1 Satz 1 SGB X).

§ 35 Abs. 1 bis Abs. 3 SGB I

(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 Zehntes Buch) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis).

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

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

§ 67 Abs. 1 S. 1 SGB X

Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.

In diesen Fällen bedarf es einer Entbindung des Mitarbeiters des Sozialamts von der Schweigepflicht gegenüber den ehrenamtlichen Helfern.

3.3.4
Datenübermittlung einer Gewerbeuntersagung

Informationen zu Gewerbeuntersagungen wegen Unzuverlässigkeit dürfen an andere öffentliche Stellen weitergegeben werden, wenn Anhaltspunkte vorliegen, dass das von der Untersagung betroffene Unternehmen trotz der Gewerbeuntersagung weiterhin sein Gewerbe z. B. in einem benachbarten Bundesland ausübt.

Der Mitarbeiter einer Kreisverwaltung wandte sich mit folgender Fragestellung an meine Dienststelle: Eine kreisangehörige Gemeinde hatte gegenüber einem im Kreis angesiedelten Bewachungsunternehmen eine Gewerbeuntersagung wegen Unzuverlässigkeit ausgesprochen. Die Unzuverlässigkeit bestand darin, dass das Unternehmen Steuern hinterzogen hatte. Den Mitarbeitern der Kreisverwaltung war bekannt, dass das Bewachungsunternehmen trotz der Gewerbeuntersagung weiterhin seine Dienste anbot. So war es unter anderem im Nachbarland Baden-Württemberg mit der Bewachung von Museen und Asylbewerberunterkünften beauftragt. Die Kreisverwaltung begehrte deshalb Auskunft, ob sie berechtigt sei, die Tatsache der Gewerbeuntersagung an die zuständigen Behörden in Baden-Württemberg zu übermitteln.

Ich habe diese Übermittlung gestützt auf § 11 Abs. 5 Satz 2 GewO für zulässig gehalten.

§ 11 Abs. 5 GewO

Öffentliche Stellen, die an gewerberechtlichen Verfahren nach Absatz 1 Satz 1 auf Grund des Absatzes 1 Satz 2, des § 35 Absatz 4 oder einer anderen gesetzlichen Vorschrift beteiligt waren, können über das Ergebnis informiert werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Diese und andere öffentliche Stellen sind zu informieren, wenn auf Grund einer Entscheidung bestimmte Rechtsfolgen eingetreten sind und die Kenntnis der

Daten aus der Sicht der übermittelnden Stelle für die Verwirklichung der Rechtsfolgen erforderlich ist. Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden oder hätten übermittelt werden dürfen. Für die Weitergabe innerhalb der zuständigen öffentlichen Stelle gelten die Übermittlungsregelungen der Sätze 1 bis 4 entsprechend.

Aufgrund der Gewerbeuntersagung durch die hessische Gemeinde war es dem von der Untersagung betroffenen Unternehmen nicht mehr erlaubt, als Bewachungsunternehmen tätig zu sein. Gleichwohl war das Unternehmen im Auftrag öffentlicher Stellen des Landes Baden-Württemberg weiterhin in dieser Funktion tätig. Aus Sicht der hessischen Kreisverwaltung war die Übermittlung der Daten an die Auftrag gebenden öffentlichen Stellen in Baden-Württemberg zur Verwirklichung der Rechtsfolgen aus der Gewerbeuntersagung damit erforderlich. Ich habe deutlich gemacht, dass die Nutzung der Daten beim Empfänger einer strikten Zweckbindung unterliegt.

3.3.5
Fehlerhafte Versendung von Mahnungen eines Zweckverbandes

Vor Datenschutzverletzungen durch menschliches Versagen muss man sich durch stichprobenhafte Kontrollen eines Arbeitsergebnisses z. B. vor seiner Versendung schützen.

Ein Bürger übersandte mir eine Mahnung zur datenschutzrechtlichen Prüfung, die auf der Rückseite die Mahnung für eine weitere Person enthielt.

Meine Rückfrage bei dem Zweckverband ergab, dass die fehlerhafte Versendung der Mahnbescheide dort bereits bekannt war. Für die Buchhaltungsabteilung werden Mahnungen seit vielen Jahren von einer Drittfirma im Rahmen einer Auftragsdatenverarbeitung nach § 4 HDSG ausgedruckt. Ein Mitarbeiter dieser Firma hatte vergessen, vor dem Ausdruck der Mahnbescheide die Duplex-Funktion des Druckers auszuschalten. Da jeder Mahnbescheid auf eine Papierseite passt, wurde faktisch nur jede zweite Mahnung verschickt, dann aber immer gleich für zwei unterschiedliche Personen.

Die im Auftrag des Zweckverbandes beschäftigte Firma wurde vom Zweckverband abgemahnt. Gleichzeitig wird die Buchhaltungsabteilung künftig bei jeder Beauftragung explizit auf die Abschaltung der Duplex-Funktion hinweisen. Darüber hinaus wurde die Firma

schriftlich dazu verpflichtet, künftig die Ausdrucke des Mahnlaufes vor der Versendung stichprobenhaft zu prüfen.

Für den fehlerhaften Mahnlauf war es einfach festzustellen, wem noch keine Mahnung zugestellt wurde. Gleichzeitig erhielten alle Empfänger der „Doppelmahnungen“ ein Entschuldigungsschreiben.

Die Datenschutzverletzung war auf menschliches Versagen zurückzuführen. Da die betroffene Stelle sich unverzüglich um eine Beseitigung des Problems – auch für die Zukunft – bemüht hat, habe ich von einer Beanstandung nach § 27 HDSG abgesehen.

3.3.6
Registrierung der Teilnahme an freiwilligen Bürgerbefragungen zwecks Versand von Erinnerungsschreiben

Im vergangenen Jahr habe ich mich mit der Frage befasst, ob bei freiwilligen Bürgerbefragungen von öffentlichen Stellen die Teilnahme/Nichtteilnahme registriert werden darf. Hintergrund hierfür waren Erinnerungsschreiben, die der Eingebende trotz eines Verzichts auf eine Teilnahme erhalten hat.

3.3.6.1
Ausgangslage

Der Magistrat der Stadt Wiesbaden führte Ende 2014 eine Bürgerumfrage zum Thema „Leben in Wiesbaden“ durch. Die Stichprobe wurde durch ein Zufallsverfahren gezogen. Die Teilnahme an der Befragung war freiwillig. Mit der Umfrage sollten allgemeine Erkenntnisse zur Zufriedenheit der Bürger mit ihrer persönlichen Lebens- und Wohnsituation gewonnen werden. So wurde beispielsweise gefragt, ob in den vergangenen zwei Jahren bestimmte Schwimmbäder besucht und wie diese bewertet wurden. Ebenso enthielt der Fragebogen aber auch Fragen zu den Themen politisches Interesse, Gesundheitsversorgung sowie Zusammenleben und Integration.

Der Eingebende, der sich gegen eine Teilnahme an dieser Umfrage entschlossen hatte, erhielt etwa zwei Wochen später ein Schreiben des Magistrats der Stadt Wiesbaden mit dem Betreff „Erinnerung an die Bürgerumfrage Leben in Wiesbaden“. Darin wurde erneut darum

gebeten, den Fragebogen auszufüllen, damit mit der Umfrage ein aussagekräftiges Ergebnis erzielt werden könne. Zugleich enthielt der Brief den Hinweis, dass das Schreiben als gegenstandslos betrachtet werden könne, falls man den Fragebogen bereits ausgefüllt und zurückgeschickt habe.

Aus Sicht des Eingebenden wurde durch dieses Schreiben eine besondere Drucksituation erzeugt, welche die Freiwilligkeit in Frage stellen könne. Zudem wurde die Frage aufgeworfen, ob tatsächlich registriert wurde, ob der entsprechende Haushalt bislang an der Umfrage teilgenommen hat oder nicht.

3.3.6.2
Ergebnis

In meiner Korrespondenz mit dem Magistrat habe ich diesen zunächst darüber aufgeklärt, dass die Tatsache, ob jemand an einer Befragung teilgenommen hat oder nicht, ein personenbezogenes Datum ist, das bei freiwilligen Umfragen nicht verarbeitet werden darf.

Auf meine Frage zum konkreten Verfahren teilte man mir mit, dass man den Befragten einen Zugangscode zugeteilt habe. Dieser wurde als Serienbriefelement in den Fragebogen und das Anschreiben aufgedruckt. Um die Erinnerungsaktion effizient zu gestalten und Druck- und Portokosten zu sparen, wurde anhand der Zugangscodes registriert, ob eine Antwort eingetroffen ist oder nicht. Dies sei jedoch datentechnisch und personell getrennt organisiert von der Erfassung der Antworten auf dem Fragebogen.

Ich habe dem Magistrat mitgeteilt, dass durch dieses Verfahren zugleich Rückschlüsse darauf möglich waren, dass die Anschreiben, über deren Zugangscode keine Rückmeldung erfolgte, nicht an der Befragung teilgenommen hatten. Nach meinem Verständnis wurden dann spätestens für die Erinnerungsschreiben wieder die Zugangscodes mit den Ausgangsadressen in Verbindung gebracht, so dass von einem personenbezogenen Datum auszugehen war.

Somit wurde tatsächlich ein Verfahren gewählt, das aus meiner Sicht datenschutzrechtlich unzulässig ist, sofern es sich um freiwillige Befragungen handelt. Da für die vergangene Befragung keine Korrektur mehr möglich war, habe ich den Magistrat darum gebeten, darauf zu achten, dass bei künftigen Befragungen von einem solchen Verfahren abgesehen wird.

Aus datenschutzrechtlicher Sicht bleibt es jedoch zulässig, wenn alle Haushalte mit einem Erinnerungsschreiben angeschrieben werden. Dieses Verfahren ist jedenfalls nicht per se dazu geeignet, die Freiwilligkeit der Umfrage in Frage zu stellen. Aus datenschutzrechtlicher Sicht ist es jedoch wünschenswert, wenn auch dem zweiten Schreiben noch einmal ein Hinweis auf die Freiwilligkeit zu entnehmen ist.

3.4
Schulen und Hochschulen

3.4.1
Datenschutzrechtliche Aspekte bei der Einführung eines Forschungsinformationssystems an hessischen Hochschulen

Die Einführung eines Forschungsinformationssystems (FIS) bedarf hinsichtlich der Verwendung von personenbezogenen Daten der Wissenschaftlerinnen und Wissenschaftler einer Rechtsgrundlage. Zudem ist es erforderlich, sich bei der Erstellung eines gemeinsamen „HeFIS-Kerndatenmodells“ auf die für ein funktionierendes und aussagefähiges Informationssystem notwendigen Daten zu beschränken.

3.4.1.1
Projektorganisation

Sieben hessische Universitäten und Hochschulen haben eine Projektorganisation aus der Taufe gehoben, welche ein Konzept für den Betrieb eines Forschungsinformationssystems entwickeln und umsetzen soll. Bei den Einrichtungen handelt es sich um die Justus-Liebig-Universität Gießen (JLU Gießen), die Hochschule Fulda (HS Fulda), die Technische Hochschule Mittelhessen, die Frankfurt University of Applied Sciences, die Hochschule Geisenheim, die Philipps-Universität Marburg sowie die Universität Kassel.

Neben der Projektleitung wurde ein Lenkungsausschuss installiert, der die Arbeit verschiedener Arbeitsgruppen koordiniert. Dabei handelt es sich um den HeFIS-Projektbeirat sowie die Arbeitsgruppen Koordination, Interessenvertretungen sowie Kommunikation.

3.4.1.2
Inhaltlicher Ansatz

Warum nun ein (einheitlich gestaltetes) Forschungsinformationssystem? Jede Hochschule ist zum einen verpflichtet, regelmäßig Berichte an das zuständige Ministerium zu liefern, um den gesetzlichen Berichtspflichten zu genügen und die Qualität von Wissenschaft und Forschung an der Einrichtung validierbar zu machen. Zum anderen gilt es, Drittmittelgeber

über den Einsatz und die Verwendung erhaltener Forschungsgelder zu informieren. Nicht zuletzt sollen die Wissenschaftlerinnen und Wissenschaftler ihre universitären Profile innerhalb und außerhalb der Einrichtung zugänglich machen, um so u. a. auf die Qualität ihrer Forschung aufmerksam zu machen. Dabei handelt es sich z. B. um Adress- und Kommunikationsdaten, Publikationen, Projekte, Angaben zu bezogenen Drittmitteln u. a. mehr. Genau hier liegt der datenschutzrechtliche Ansatzpunkt: Personenbezogene Daten der Betroffenen sollen in ein Informationssystem eingestellt und der Öffentlichkeit zugänglich gemacht werden.

3.4.1.3
Organisatorisch-technischer Ansatz

Zunächst ist vorgesehen, ein gemeinsam definiertes Kerndatenmodell zu entwickeln, welches an allen beteiligten Universitäten und Hochschulen zur Anwendung kommt. Dieses stützt sich auf den Kerndatensatz Forschung (dieser beschreibt, welche Angaben Universitäten, Fachhochschulen, außeruniversitäre Forschungseinrichtungen und andere forschende Einrichtungen zu ihren Forschungsaktivitäten bereithalten sollen). Jede beteiligte Einrichtung soll den gemeinsamen Kern erweitern können. Als Ergebnis sollen gemeinsame Strukturen geschaffen werden, die es ermöglichen, forschungsbezogene Daten durch die Implementierung von Standardmodellen zu harmonisieren, dezentrale Bestände an Forschungsdaten zusammenzuführen, die Datenerfassung und Datenpflege zu vereinfachen sowie eine Stärkung der Wahrnehmung und Sichtbarkeit des Forschungsprofils der Hochschulen in Wissenschaft und Öffentlichkeit zu erreichen.

Hierfür sollten (personenbezogene) Daten der Wissenschaftlerinnen und Wissenschaftler aus verschiedenen bereits vorhandenen Datenbanken entnommen und zum Aufbau eines FIS verwendet werden. So war geplant, u. a. personenbezogene Daten aus SAP/OpenLDAP (Personal) bzw. SAP/HIS (Studenten) in eine neu aufzubauende, für ein FIS zur Verfügung stehende Datenbank einzuspielen. Hinzu sollten Finanzdaten, Daten der Drittmittelverwaltung, Publikationsdaten, Organisationsdaten u. a. kommen, um so ein inhaltlich umfangreiches Informationssystem aufzubauen.

Erste Testinstallationen an zwei Einrichtungen (JLU Gießen und HS Fulda) wurden implementiert. Hierzu wurden auch Verfahrensverzeichnisse erstellt, da für die Testung auch personenbezogene Daten verwendet wurden. Ich hatte diesem Vorhaben seinerzeit unter Auflagen zugestimmt.

3.4.1.4
Rechtliche Grundlagen für den Betrieb eines FIS

Neben den technischen und organisatorischen Herausforderungen des Projekts hat sich nicht zuletzt die Frage nach einer Rechtsgrundlage gestellt, um personenbezogene Daten z. B. aus den einschlägigen SAP-Modulen heraus in eine neu zu schaffende Datenbank zu exportieren und für ein FIS zu verwenden.

Die betroffenen Hochschulen waren zunächst der Auffassung, dass § 34 HDSG hierfür in Betracht kommen könnte.

§ 34 Abs. 1 Satz 1 HDSG

(1) Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht.

In einer vom HeFIS-Verbund angeforderten Stellungnahme hierzu habe ich mitgeteilt, dass ich in § 34 HDSG keine ausreichende Rechtsgrundlage erkennen könne und eine bereichsspezifische Regelung erforderlich sei. Dies vor allem unter dem Aspekt, dass § 34 HDSG keine Änderung des Erhebungszwecks vorsehe und die dort genannten Kriterien für die Verwendung der Daten in einem FIS nicht einschlägig und daher abschließend seien. In diesem Zusammenhang verwies ich auf meine Stellungnahme gegenüber dem Hessischen Ministerium für Wissenschaft und Kunst zur Novellierung des Hessischen Hochschulgesetzes (s. a. Ziff. 3.1.2). Durch eine Ermächtigungsnorm zur Datenerhebung im Hochschulgesetz und der Konkretisierung in Form einer Rechtsverordnung, die ich empfohlen habe, kann die Datenerhebung bzw. deren Verwendung aus anderen Systemen heraus legitimiert werden.

Nach der Verabschiedung des Gesetzes muss das Ministerium in Abstimmung mit den Hochschulen eine Rechtsverordnung erlassen, in welcher u. a. der Rahmen für die Verwendung personenbezogener Daten gesetzt wird.

3.4.2
Datenschutzrechtliche Anforderungen an den Betrieb eines SharePoints am Beispiel einer Förderschule

Personenbezogene Daten in einer Cloud zu speichern, hat sich mittlerweile etabliert. Auch der Einsatz von SharePoint verbreitet sich zunehmend. Davon sind Schulen nicht ausgenommen. Datenschutzrechtlich ist eine derartige Anwendung dann akzeptabel, wenn erforderliche technische und organisatorische Sicherheitsmaßnahmen umgesetzt sind.

3.4.2.1
Vorbemerkung

SharePoint ist eine Webanwendung (von Microsoft), die unter anderem folgende Anwendungsgebiete abdeckt:

– Zusammenarbeit, beispielsweise das Verwalten von Projekten oder die Koordination von Aufgaben,
– Soziale Netzwerke, z. B. über persönliche Webseiten, Team-Webseiten, Diskussionsgruppen und Blogs,
– Intranetportale,
– Content-Management über Dokumentenmanagement-Funktionen, Inhaltsverwaltung, Metadaten und benutzerangepasste Suchfunktionen,
– Geschäftsanwendungen.

Es besteht jedoch für die Anwender auch die Möglichkeit, einen anderen Dienstleister (z. B. den Schulträger selbst) einen SharePoint betreiben zu lassen. Notwendig hierzu ist der Aufbau erforderlicher personeller und sachlicher Ressourcen. Durch die Nutzung einer interaktiven Plattform, in welche u. a. Fachliteratur eingestellt, ein Terminkalender geführt oder aber Kommunikation betrieben werden kann, können Lehrkräfte ihre zeitlichen Ressourcen besser nutzen. Dies erscheint gerade für sog. Flächenkreise ein enormer Vorteil zu sein.

Datenschutzrechtliche Aspekte müssen dann Berücksichtigung finden, soweit auf der Plattform personenbezogene Daten eingestellt und verarbeitet werden. Dabei handelt es sich in der Regel um Daten von Lehrkräften, Schülern und Eltern.

3.4.2.2
Art der zu verarbeitenden personenbezogenen Daten

Bei den Daten, die von Förderschulen erhoben und verarbeitet werden, handelt es sich neben den klassischen Stammdaten der Schüler und Eltern (z. B. Name, Anschrift, Geburtsdatum etc.) auch um spezifische Daten, welche im Rahmen der Erstellung von Förderlisten und Förderplänen verarbeitet werden.

3.4.2.2.1
Förderlisten

Diese Unterlagen enthalten Grundangaben zum Schüler; u. a. den Hinweis, dass er eine Fördermaßnahme benötigt oder eine solche erhält.

3.4.2.2.2
Förderpläne

Diese Unterlagen enthalten Angaben über konkrete Fördermaßnahmen, die für den betroffenen Schüler vorgesehen sind. Aus der Beschreibung der geplanten Maßnahmen ergibt sich in der Regel das Defizit, welchem – im Sinne des Betroffenen – entgegengewirkt werden soll.

3.4.2.2.3
Adress- und Kontaktlisten von Ärzten, Psychotherapeuten und Apotheken

Nicht in den SharePoint gehören besonders sensitive Daten, wie sie z. B. in einem förderdiagnostischen Gutachten enthalten sind. Bei der Erstellung derartiger Gutachten werden z. B. auch Familienanamnesen, körperliche Defizite des Schülers, Defizite des Sozialverhaltens u. a. erhoben. Solche Angaben sind durch die Förderlehrkraft separat unter Beachtung der einschlägigen Maßnahmen zu Datensicherheit sowie des Zugriffsschutzes aufzubewahren. Im Übrigen gelten auch für deren dienstliche Tätigkeit im häuslichen Bereich die Rahmenbedingungen, die in der Vereinbarung zur dauerhaften Einführung alternierender Telearbeit im Bereich der Hessischen Landesverwaltung festgelegt sind.

3.4.2.3
Technische Ausgestaltung

Zunächst ist festzulegen, ob man sich der Dienste privater Dritter (klassischer Cloud-Anbieter) bedient oder eher eine „interne" Lösung bevorzugt. Interne Lösung heißt, dass z. B. der Schulträger als Betreiber des SharePoints fungiert und damit auch den Support gewährleistet.

3.4.2.3.1
Support

Dieser muss, insbesondere hinsichtlich der Administration (Verfügbarkeit), jederzeit gewährleistet sein.

3.4.2.3.2
Datenübertragung

Der Zugang zum Server muss verschlüsselt sein. Ein höherer Sicherheitsstandard wird durch reine Zwei-Faktor-Authentifizierung (Token) erreicht. Eine andere Möglichkeit ist der Aufbau eines VPN-Tunnels zwischen Client und Server. Die Umsetzung derartiger Maßnahmen erhöht den Schutz der Daten erheblich und ist grundsätzlich anzustreben. Allerdings sind derartige Lösungen nicht zwingend, sondern als beispielhaft anzusehen. Auch andere, technische Alternativen können in eine nähere Betrachtungsweise einbezogen werden.

3.4.2.3.3
Arbeitsplätze (Endgeräte)

Die grundsätzliche Problematik der Nutzung privater Endgeräte für dienstliche Zwecke ist nach wie vor vorhanden. Vor allem im Zusammenhang mit der Verarbeitung besonders sensitiver Daten (z. B. Gesundheitsdaten) sind die Anforderungen an die Datensicherheit und den Zugriffsschutz am häuslichen Arbeitsplatz der Lehrkraft besonders anspruchsvoll.

Deshalb ist es unabdingbar, dass für den Transport und die Speicherung der Daten nur Speichermedien verwendet werden, die mit einer nach dem Stand der Technik aktuellen Schutzsoftware ausgerüstet sind.

Der Problematik hinsichtlich der Nutzung (privater) mobiler Endgeräte durch die Lehrkräfte ist mit der Nutzung eines Device Management zu begegnen. Bestimmte Betriebssysteme werden dadurch für eine Kommunikation mit dem betroffenen Server gesperrt. Auch ist die Realisierung einer GeoIP-Sperre mittels einer zweiten, nachgeschalteten Firewall sinnvoll, die Zugriffsversuche, die von außerhalb der Bundesrepublik Deutschland erfolgen, abblockt.

3.4.2.4
Rollen- und Berechtigungskonzept

Einer der Kernpunkte des Datenschutzrechts befasst sich mit der Frage des Zugriffs auf personenbezogene Daten. Dahinter verbirgt sich der Grundsatz, dass jeder nur auf die ihn betreffenden, dienstlichen Daten Zugriff haben soll. Für Lehrer heißt das, dass der Zugriff auf die Schülerdaten der eigenen Klasse ermöglicht ist und, soweit dies erforderlich ist bzw. notwendig wird, der (temporäre) Zugriff auf die Daten der z. B. Vertretungsklasse ermöglicht wird.

In diesem Zusammenhang stellt sich immer wieder die Frage nach einem angemessenen Rollen- und Berechtigungskonzept. Dabei ist durch die Administration (hier: Schulleitung) sicherzustellen, dass die Lehrkräfte ausschließlich auf die Daten (der Schülerinnen und Schüler) Zugriff haben, für die sie verantwortlich sind. Der Umfang der Berechtigungen hat sich an der funktionalen Stellung des Zugriffsberechtigten auszurichten. So hat die Schulleitung ohne Zweifel umfangreichere Berechtigungen als die einzelne Lehrkraft an dieser Schule.

3.4.2.5
Passwort und Passwortwechsel

Die Vergabe eines Passwortes dient der Übertragung persönlicher Verantwortung. Mittlerweile ist durch die Rechtsprechung bestätigt, dass alle Systemaktivitäten eines Nutzers, welche mit seinem persönlichen Passwort initiiert wurden, diesem auch unmittelbar zugerechnet werden. Umso wichtiger ist es, ein ausreichend sicheres und in regelmäßigen

Abständen erneuertes persönliches Passwort zu verwenden. Ein regelmäßiger Passwortwechsel im Zusammenhang mit dem LOGIN ist für jeden Anwender zwingend. Es muss mindestens acht Stellen lang sein und mit Groß- und Kleinbuchstaben sowie Sonderzeichen befüllt werden. Ein Passwortwechsel in einem Zeitraum von 45 bis 60 Tagen erscheint angemessen. Im Rahmen der Empfehlungen des Bundeamtes für die Sicherheit in der Informationstechnik kann ein Zeitraum gewählt werden, welcher zur Überbrückung der Sommerferien geeignet ist. Das Passwort muss durch den Anwender selbst bestimmt werden und darf auch nur diesem bekannt sein. Ausnahmen bilden die für Notfälle hinterlegten Zugangsinformationen, deren Nutzung dokumentiert und begründet sein muss.

3.4.2.6
Protokollierung

Protokollierungsfunktionen sind systemseitig zu gewährleisten. Dabei ist sicherzustellen, dass systemrelevante Aktivitäten nutzerbezogen erfasst und über einen bestimmten Zeitraum gespeichert werden. Die Aufbewahrungsdauer (Speicherdauer) der Protokolldateien hat sich am Maßstab der „Erforderlichkeit im Rahmen der Aufgabenerfüllung" auszurichten. Der Zeitraum für die Speicherung selbst kann je nach Erfordernis auf mehrere Tage bis zu einigen Monaten festgelegt werden.

3.4.2.7
Löschung

Die Löschung der Daten hat sich auszurichten an ggfs. spezialgesetzlichen Regelungen einerseits und dem Grundsatz der Zweckerfüllung andererseits (s. a. § 19 Abs. 3 HDSG). Danach sind personenbezogene Daten unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind.

3.4.2.8
Zusammenfassung

An den Betrieb und Support eines SharePoints sind unter datenschutzrechtlichen Gesichtspunkten folgende Bedingungen geknüpft:

– Zunächst ist die grundsätzliche Entscheidung zu treffen, ob ein privater Dienstleister (Cloud-Anbieter) beauftragt wird oder z. B. der Schulträger für die Dienstleistung zur Verfügung steht.
– Es sind administrativ-organisatorische Festlegungen hinsichtlich der zu speichernden, personenbezogenen Daten zu treffen. Auszuschließen ist u. a., dass förderdiagnostische Gutachten im SharePoint abgelegt werden.
– Auf die Zukunft ausgerichtet ist anzustreben, die Datenübertragung über eine HTTPS-Verschlüsselung hinaus noch sicherer zu machen.
– Die Nutzung zertifizierter Arbeitsplätze ist (als Fernziel) ebenfalls anzustreben.
– Die Sperrung (privater) mobiler Endgeräte für eine Nutzung des SharePoints ist unumgänglich.
– Die Einrichtung einer GeoIP-Sperre ist gleichermaßen anzustreben.
– Die Erstellung eines Rollen- und Berechtigungskonzepts ist zwingend.
– Die Einrichtung eines mind. achtstelligen persönlichen Passwortes für jede Lehrkraft ist unabdingbar. Ein regelmäßiger Passwortwechsel ist technisch-administrativ umzusetzen.
– Eine Systemprotokollierung ist einzurichten (weitere Informationen sind der „Orientierungshilfe Protokollierung" der Datenschutzbeauftragten von Bund und Ländern zu entnehmen).
– Die Löschung der personenbezogenen Daten nach den gesetzlichen Vorgaben (Spezialgesetz oder allg. HDSG) ist zu gewährleisten.

3.4.3
Datenschutz und wissenschaftliche Forschung an Schulen

Die wissenschaftliche Forschung an Schulen ist etabliert und wichtig, um nicht ausschließlich schulbezogene Entwicklungen erkennen und darauf angemessen reagieren zu können. Deshalb ist die Datenerhebung für diesen Zweck in § 84 des Hessischen Schulgesetzes (HSchG) normiert. Art, Umfang und Ausgestaltung derartiger Forschung sind mit Vorgaben verbunden, für die der Gesetzgeber detaillierte Verfahrensschritte formuliert hat.

3.4.3.1
Rechtliche Voraussetzungen

Wissenschaftliche Forschung an den hessischen Schulen hat Konjunktur. Neben großen, internationalen und nationalen Studien wie PISA (Internationale Schulleistungsuntersuchungen), IQB-Ländervergleich (Überprüfung von Bildungsstandards) oder NEPS (National Educational Panel Study) werden auch eine Fülle teilweise regional bezogener Forschungsvorhaben, z. B. von bestimmten Fachbereichen einzelner Universitäten, an ausgewählten Schulen durchgeführt.

Rechtsgrundlage hierfür ist § 84 HSchG.

§ 84 HSchG

(1) Wissenschaftliche Forschungsvorhaben in Schulen bedürfen der Genehmigung des Kultusministeriums; die Befugnis kann auf die Schulaufsichtsbehörden übertragen werden. Die Genehmigung erziehungswissenschaftlicher Forschungsvorhaben soll erteilt werden, wenn die Erfüllung des Bildungsauftrages der Schule hierdurch nicht unangemessen beeinträchtigt wird. Vor Erteilung der Zustimmung ist die Schulkonferenz zu hören. Die Genehmigung von Forschungsvorhaben, bei denen personenbezogene Daten verarbeitet werden, ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Personenbezogene Daten dürfen für ein bestimmtes wissenschaftliches Forschungsvorhaben in der Regel nur mit Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler verarbeitet werden. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Personenbezogene Daten dürfen ohne Einwilligung der Betroffenen verarbeitet werden, soweit deren schutzwürdigen Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden. Der Einwilligung der Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die Betroffenen sind darauf hinzuweisen, dass sie die Einwilligung ohne Rechtsnachteile verweigern können; sie sind dabei über das Ziel und den wesentlichen Inhalt des Forschungsvorhabens, die Art ihrer Beteiligung an der Untersuchung sowie die Verarbeitung der erhobenen Daten aufzuklären. § 33 Abs. 2 und 3 des Hessischen Datenschutzgesetzes gilt entsprechend.

3.4.3.2
Praktische Umsetzung

3.4.3.2.1
Beteiligte Stellen

Welche Bedeutung haben nun die rechtlichen Vorgaben des § 84 HSchG in der praktischen Anwendung? Zunächst geht es um die Frage, wer für das Genehmigungsverfahren zuständig ist. Hier hat der Gesetzgeber das Kultusministerium vorgesehen, welches die Befugnis auf die Schulaufsichtsbehörden, also die Staatlichen Schulämter, übertragen kann. Von dieser Möglichkeit hat das Ministerium bislang keinen Gebrauch gemacht. Es ist daher die zuständige Stelle für die Erteilung von Genehmigungen im Zusammenhang mit wissenschaftlicher Forschung an Schulen. Die Erteilung von Genehmigungen erziehungswissenschaftlicher Forschungsvorhaben soll (einschränkend) erteilt werden, wenn dadurch die Erfüllung des Bildungsauftrags der Schule nicht unangemessen beeinträchtigt wird. Deshalb muss vor der Erteilung der Zustimmung die Schulkonferenz hierzu gehört werden. Schließlich ist der Hessische Datenschutzbeauftragte bei Forschungsvorhaben mit Personenbezug in Kenntnis zu setzen.

3.4.3.2.2
Einwilligung der Betroffenen und Informationspflichten

Wie für jede Verarbeitung personenbezogener Daten gilt als Ermächtigungsgrundlage nur ein Gesetz oder aber die Einwilligung der Betroffenen. Auch die Form der Einwilligung ist klar vorgegeben: Sie hat schriftlich zu erfolgen. Ausnahmen von der Schriftform sind nur wegen besonderer Umstände möglich, die wohlbegründet und nachvollziehbar sein müssen. Von einer Einwilligung kann nur abgesehen werden, soweit hinsichtlich der schutzwürdigen Belange der Betroffenen folgende Voraussetzungen vorliegen: Die Art der Daten, deren Offenkundigkeit sowie die Art ihrer Verwendung führen zu dem Ergebnis, dass das Persönlichkeitsrecht der zu Befragenden nicht unzulässig eingeschränkt wird. Die Informationspflichten der datenerhebenden Stelle sind ebenfalls klar definiert. So sind die Betroffenen darüber in Kenntnis zu setzen, dass sie die Einwilligung ohne Rechtsnachteile verweigern können, sowie darüber aufzuklären, welches Ziel die Datenerhebung verfolgt, welche Inhalte das Forschungsvorhaben hat, in welcher Weise die Betroffenen daran mitwirken sollen und schließlich wie die erhobenen Daten verarbeitet werden.

3.4.3.3
Konkreter Ablaufplan und Datenschutzkonzept sind erforderlich

Immer wieder zeigt sich, dass an verschiedenen Stellen des Verfahrens zur Durchführung wissenschaftlicher Forschungsprojekte an Schulen Defizite auch und insbesondere im Hinblick datenschutzrechtlicher Aspekte auftreten. Denn die angemessene Information der Betroffenen über das Projekt z. B. hinsichtlich der Datenverarbeitung ist Bestandteil eines plausiblen und nachvollziehbaren Datenverarbeitungskonzepts.

Zunächst hat die datenerhebende Stelle ein Forschungsdesign zu erstellen. Neben dem Ziel der Erhebung und den Auswahleinheiten (konkrete Schulen/Klassen bestimmter Jahrgangsstufen etc.) sind die zuständigen Ansprechpartner zu benennen. Daneben sollte ein konkreter Ablaufplan hinsichtlich der Inhalte und der Zeiträume erstellt sein. Ebenso ist ein Datenverarbeitungskonzept erforderlich, in dem der Ablauf des maschinellen Datenverarbeitungsverfahrens geschildert wird. Bestandteil der Unterlagen muss selbstverständlich auch der Fragebogen sein, welcher verwendet wird. Handelt es sich um eine Online-Erhebung, sind die technischen Voraussetzungen und vorgesehene Datensicherheitsmaßnahmen (z. B. Passwort, Verschlüsselung etc.) zu schildern. Nicht zuletzt sollte zu diesem Zeitpunkt bereits auch ein Informationsschreiben an die Betroffenen formuliert sein, in dem u. a. die in § 84 Abs. 2 HSchG beschriebenen Inhalte aufgenommen sind. Hinzu kommen die Informationen zur Löschung der Daten nach dem Ende der Datenauswertung sowie der Umgang mit den Fragebogen (Stichwort: datenschutzgerechte Vernichtung). Mit diesen Unterlagen tritt die datenerhebende Stelle an die Schule und das Ministerium heran. Schließlich muss unabhängig von der Genehmigung durch das Ministerium die Schule bzw. die Schulleitung von der Notwendigkeit des Verfahrens überzeugt sein.

Sind diese Hürden genommen, gilt es Eltern und Schüler zu überzeugen. Dies gelingt dann, wenn hinsichtlich der Transparenz des Verfahrens keine Wünsche der Betroffenen offenbleiben. Dies sicherzustellen ist eine wesentliche Voraussetzung für die erforderliche Akzeptanz, um eine möglichst hohe Beteiligung sicherzustellen und damit valide Ergebnisse zu erzielen.

3.4.4
Videoüberwachung in der Schule auch 2015 im Fokus

Nach wie vor steht das Thema Videoüberwachung auf der Agenda von Schulleitern und Schulträgern. An den rechtlichen Voraussetzungen hierfür, die aus dem Polizeirecht abgeleitet werden müssen, hat sich ebenso wenig geändert wie meine Hinweise, dass dieses Instrumentarium nur „das letzte Mittel" sein kann, um Einbruch, Vandalismus oder Gewaltdelikte in den Griff zu bekommen. Im konkreten Fall der „Schule Obersberg" habe ich entsprechend den Wünschen des Schulträgers und der Schule vor Ort beraten und zusammen mit dem Landkreis Hersfeld-Rotenburg ein Konzept verabschiedet, welches sowohl dem Anliegen der Schule als auch des Datenschutzes gerecht wird.

3.4.4.1
Die Ausgangssituation

Mit dem Thema „Videoüberwachung" an Schulen ist mein zuständiger Mitarbeiter jedes Jahr intensiv befasst. Von den zahlreichen Anfragen von Schulleitern oder Schulträgern muss ein guter Teil abschlägig beschieden werden. Im Fall des Landkreises Hersfeld-Rotenburg kam es im Jahr 2013 zu umfangreichen Aktivitäten meines Hauses hinsichtlich der Videoüberwachung an fünf Schulen (s. a. 42. Tätigkeitsbericht, Ziff. 3.3.5.2). Der Landrat des Landkreises stattete meiner Dienststelle nun einen Besuch ab, um sich über neu geplante Maßnahmen zur Überwachung des Campus einer Schule mit mir abzustimmen.

Die Schule liegt abseits des Stadtzentrums auf einer Anhöhe. Die verschiedenen Gebäude des Campus werden von einem bewaldeten Gelände eingeschlossen. Zudem ist das Gelände unübersichtlich, das Gebäude der Gesamtschule sowie der damit verbundenen Oberstufe verschachtelt. Das Gebäude der kaufmännischen Berufsschule ist separat und war nicht Gegenstand von geplanten Maßnahmen. Auf dem Campus befindet sich zusätzlich ein neu erbautes AudiMax mit Mensa. Mehr als 2000 Schülerinnen und Schüler bewegen sich tagsüber auf dem Gelände. Hinzu kommen diverse Vereine der Stadt, welche die Schwimmhalle und die Sporthalle für Training und Wettkampf nutzen. Von morgens um 6:00 Uhr bis abends um 22:00 Uhr sind die Türen der Schule deshalb geöffnet. Entsprechend unübersichtlich sind die baulichen und nutzerbezogenen Verhältnisse. Wiederholt kam es in der Vergangenheit zu Diebstählen, Vandalismus (z. B. am neu erbauten AudiMax) und Manipulationen an Bremsanlagen von Fahrrädern. Diese hätten besonders fatal für die Betroffenen enden können, müssen die Schüler doch auf dem Weg nach Hause eine ausgedehnte Gefällstrecke befahren. Schüler, Lehrer und Eltern forderten seit geraumer Zeit eine Videoüberwachung, auf welche die Kreisverwaltung nun eingehen

wollte, nicht ohne allerdings eine datenschutzrechtliche Expertise meines Hauses in die Realisierung der Maßnahme einzubeziehen.

3.4.4.2
Die rechtliche Beurteilung

Der Einsatz von Videokameras ist nichts anderes als eine automatisierte Form der Verarbeitung personenbezogener (Bild-)Daten. Eine spezifische rechtliche Grundlage für deren Einsatz in Schulen etwa im Schulgesetz oder in den einschlägigen Verordnungen zur Datenverarbeitung in Schulen gibt es nicht. Auch das Hessische Datenschutzgesetz hilft in diesem Fall nicht weiter. So bleibt bis auf weiteres einzig das Hessische Gesetz über die Sicherheit und Ordnung (HSOG) vom 14.01.2005 (GVBl. I S. 14), um hilfsweise den Betrieb einer Überwachungsanlage in Schulen rechtfertigen zu können.

§ 14 Abs. 1, 3 und 4 HSOG

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

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

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

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

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

Die Installation einer Videoüberwachung (nicht nur) an einer Schule ist an Bedingungen geknüpft. Um überhaupt eine derartige Datenverarbeitung rechtfertigen zu können, muss das Hessische Gesetz über die öffentliche Sicherheit und Ordnung herangezogen werden. So ist nach § 14 Abs. 2 Nr. 2 HSOG die Videoüberwachung zum Schutz einer besonders gefährdeten öffentlichen Einrichtung erlaubt. Schulen sind nicht von vornherein besonders gefährdete öffentliche Einrichtungen im Sinne des HSOG. Es reicht also nicht aus, wenn es einmal zu einem Vandalismusschaden gekommen ist. Vielmehr müssen derart schwerwiegende Beeinträchtigungen vorliegen, dass der Einsatz von Videotechnik zum Schutz der Einrichtung oder von Personen erforderlich ist und in Abwägung mit dem Rechtseingriff bei den Personen, deren Verhalten aufgezeichnet wird, verhältnismäßig erscheint.

Konkret rechtfertigt das den Einsatz der Technik dann, wenn schwere Sachbeschädigungen in dem zur Überwachung vorgeschriebenen Bereich aufgetreten sind oder aber gehäuft tätliche Angriffe gegen Dritte zu verzeichnen sind. Ebenso kann man damit besonders schweren Straftaten oder häufigen Straftaten (z. B. Drogenkriminalität) entgegenwirken. Das Bundesverwaltungsgericht hat in seinem Urteil vom 25.01.2012 (BVerwGE 141, 329) hierfür Kriterien entwickelt. Für die Beurteilung der Verhältnismäßigkeit spielt die Tiefe des Eingriffs in das Persönlichkeitsrecht der Betroffenen eine entscheidende Rolle. Der Rechtseingriff ist relativ gering, wenn z. B. die Kameras mit einer Einbruchmeldeanlage gekoppelt sind und eine Scharfschaltung außerhalb des Schulbetriebs bzw. in den Ferien erfolgt oder aber nur nachts in Betrieb ist.

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

3.4.4.3
Die Begehung vor Ort

Zu einem gemeinsamen Termin hat sich mein zuständiger Mitarbeiter nach Bad Hersfeld begeben, um vor Ort mit dem Landrat, der Schulleitung und anderen Entscheidungsträgern die Lage zu sondieren. Vier Komplexe gab es zu betrachten:

– das AudiMax
– der Fahrradständer
– die Ebene 01 der Modell- und Gesamtschule
– die Ebene 02 der Modell- und Gesamtschule.

Insgesamt sollten 32 Kameras installiert werden. Die Anzahl von Kameras insbesondere auf der Ebene 02, auf welcher sich die Sporthalle und das Schwimmbad befinden, erschien mir vor allem hinsichtlich des dort stattfindenden Schwimm- und Sportunterrichts, überdimensioniert. Zudem sollte auf jede dort befindliche Umkleidekabine eine Kamera gerichtet werden.

3.4.4.4
Das Ergebnis: Reduzierung von 32 auf 23 Kameras

Unstrittig waren die zehn vorgesehenen Kameras für die Gebäudesicherung des AudiMax. Ebenso verhielt sich das mit den vier für den Fahrradständer vorgesehenen Bildaufzeichnungsgeräten. Hinzu kamen auf der Ebene 01 (auf welcher sich der Fahrradständer befindet) zwei Kameras, welche den Eingangsbereich bzw. ein Treppenhaus überwachen sollen.

Einige Vorbehalte hatte ich gegen die ursprünglich 16 vorgesehenen Überwachungskameras auf der Ebene 02, auf der sich Schwimmhalle und Sporthalle befinden. Insbesondere die Überwachung der Zugänge zu den Umkleideräumen erschien mir überzogen zu sein. Hinzu kommt, dass zumindest teilweise der laufende Schulbetrieb in Form des Sport- und Schwimmunterrichts betroffen ist. Nach diversen Telefonaten und E-Mail-Verkehr im Nachgang zu der Besprechung in Bad Hersfeld ist die Anzahl der Aufzeichnungsgeräte drastisch auf die Anzahl von sieben gesenkt worden, ohne dadurch den Anspruch auf eine effiziente Kontrolle zu konterkarieren. Da die Investitionen für das Vorhaben haushaltsrechtlich noch im Jahre 2015 durch den Kreisausschuss getätigt werden mussten, hatte mein Mitarbeiter innerhalb von einer Woche Ende des Monats Oktober die Besichtigung vorgenommen sowie die grundsätzliche, datenschutzrechtliche Expertise gefertigt.

Das Ergebnis ist nun eine maßvolle, sich auf die neuralgischen Zonen beschränkende Videoaufzeichnung der Gebäude bzw. des Campus der Modell- und Gesamtschule Obersberg.

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

4.1
Bußgeldverfahren

4.1.1
Überblick über die im Berichtsjahr abgeschlossenen Bußgeldverfahren

Auch in diesem Jahr wurde wieder eine Vielzahl von Bußgeldverfahren anhängig. Spektakuläre Fälle waren dabei allerdings nicht zu verzeichnen.

Den zu bearbeitenden Fällen lagen auch in diesem Jahr sehr unterschiedliche Sachverhalte zugrunde.

Insbesondere im Kontext der Nichtbeachtung von Werbewidersprüchen wurden mehrmals Verfahren durchgeführt, da sich Verstöße wiederholt hatten, nachdem die Aufsichtsbehörde einen ersten Verstoß beanstandet hat, verbunden mit der Aufforderung in Zukunft größere Sorgfalt walten zu lassen. Im Rahmen der Bearbeitung stellte sich dann teilweise heraus, dass bei der Löschung der Daten nach erfolgtem Werbewiderspruch nicht sorgfältig genug vorgegangen wurde. Sei es, weil nicht alle für Werbezwecke vorgehaltenen Dateien abgeglichen wurden, sei es, dass nur einzelne E-Mail-Adressen gelöscht wurden, obwohl der Betroffene ausdrücklich die Löschung aller zu seiner Person gespeicherten Daten verlangt hatte.

Wie in den letzten Jahren berichtet, versuche ich seit einiger Zeit die Nichterfüllung der Auskunftsverpflichtung an die Aufsichtsbehörde gem. § 38 Abs. 3 BDSG mit Hilfe von Zwangsgeldandrohungen durchzusetzen. Grundsätzlich führt dies häufig dann zu zeitnahen Antworten. Allerdings schließt das im Einzelfall nicht aus, dass trotzdem auch ein Bußgeld verhängt wird. Dies betrifft insbesondere solche Fälle, in denen auch nach Nachfrage keine oder nicht vollständige Auskunft erteilt wurde. Häufig sind in diesen Fällen zudem weitere Verstöße zu ahnden, insbesondere die Nichterteilung von Auskünften an den Betroffenen oder unzulässige Datenverarbeitungen.

In diesem Jahr wurden insgesamt 30 Verfahren abgeschlossen. Dem lagen 11 Verstöße gegen Pflichten der verantwortlichen Stellen gegenüber Betroffenen und Aufsichtsbehörden

(Tatbestände des § 43 Abs. 1 BDSG) zugrunde sowie 19 Verstöße wegen unzulässiger Datenverarbeitung (Tatbestände des § 43 Abs. 2 BDSG). Insgesamt wurden 16 Bußgelder in Höhe von 14.200 EUR verhängt. In einem Fall habe ich Strafantrag gestellt.

4.1.2
Eine unzulässige Werbe-E-Mail – vier bußgeldfähige Datenschutzverstöße

E-Mail-Werbung ohne Einwilligung des Adressinhabers ist grundsätzlich unzulässig. Bei jeder Nutzung personenbezogener Daten zu Werbezwecken ist der Adressat auf sein Widerspruchsrecht hinzuweisen. Bei der Erteilung einer Auskunft an Betroffene über die zu ihrer Person gespeicherten Daten sind diese Daten immer konkret zu benennen. Wenn mehr als neun Personen in einem Unternehmen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein betrieblicher Datenschutzbeauftragter zu bestellen.

Durch die Eingabe einer Betroffenen, die sich aufgrund einer unerwünschten personalisierten Werbe-E-Mail mit einer Beschwerde an mich wandte, wurde ich auf ein hessisches Unternehmen mit sechs unselbständigen Niederlassungen im Bundesgebiet aufmerksam, bei dem sich im Laufe der Bearbeitung der Eingabe herausstellte, dass dort offensichtlich keinerlei Kenntnisse grundlegender datenschutzrechtlicher Regelungen vorhanden waren.

4.1.2.1
Intransparente Datenerhebung und E-Mail-Werbung ohne Einwilligung

Die Betroffene hatte dem Unternehmen ihre E-Mail-Adresse bereits vor Jahren anlässlich einer Terminvereinbarung überlassen und die Dienstleistung des Unternehmens seither nicht mehr in Anspruch genommen. Bei der damaligen Datenerhebung wurde sie entgegen § 4 Abs. 3 Nr. 2 BDSG nicht auf eine beabsichtigte künftige Nutzung der E-Mail-Adresse zu Werbezwecken hingewiesen.

§ 4 Abs. 3 BDSG

Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten.

Umso überraschter war sie, als sie eine E-Mail-Mitteilung des Unternehmens über den bevorstehenden Umzug einer Niederlassung erhielt, in der zusätzlich ausführlich für die Dienstleistungen und aktuelle Sonderangebote geworben wurde.

Grundsätzlich bedarf die werbliche Nutzung einer personenbeziehbaren E-Mail-Adresse gem. § 28 Abs. 3 BDSG der Einwilligung der Betroffenen.

§ 28 Abs. 3 Satz 1 BDSG

Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt.

Da im vorliegenden Fall keine der Regelungen des § 28 Abs. 3 Satz 2 bis 5 BDSG zur Anwendung kommen konnte, nach denen eine Einwilligung in die Nutzung personenbezogener Daten zu Werbezwecken bei Bestandskunden unter bestimmten Bedingungen nicht erforderlich gewesen wäre, hätte das Unternehmen die E-Mail-Adresse der Betroffenen ohne Einwilligung nicht zu Werbezwecken nutzen oder verarbeiten dürfen. Da die personenbezogene E-Mail-Adresse der Betroffenen nicht allgemein zugänglich war, erfüllte das Unternehmen mit der unbefugten Verarbeitung der E-Mail-Adresse zu Werbezwecken den Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG.

4.1.2.2
Hinweis auf das Widerspruchsrecht gegen Werbung

Bereits bei der damaligen Datenerhebung anlässlich des ersten Vertragsabschlusses hätte die Betroffene gem. § 28 Abs. 4 Satz 2 BDSG darauf hingewiesen werden müssen, dass ihr ein Widerspruchsrecht gegen die Verarbeitung der erhobenen Daten zu Werbezwecken zusteht. Dieser Hinweis wurde aber unterlassen. Zusätzlich musste ich feststellen, dass die Werbe-E-Mail entgegen § 28 Abs. 4 Satz 2 BDSG weder einen Hinweis auf das

Widerspruchsrecht gegen Werbung noch den bei Werbe-E-Mails üblichen und durchaus als Widerspruchshinweis im Sinne dieser BDSG-Vorschrift interpretierbaren Abmeldelink enthielt.

§ 28 Abs. 4 Satz 2 1. Halbsatz BDSG

Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; ...

Wer personenbezogene Daten seiner Kunden zu Werbezwecken verarbeitet und den Betroffenen bei der Datenerhebung und bei jeder werblichen Ansprache nicht auf sein Widerspruchsrecht hinweist, erfüllt den Bußgeldtatbestand des § 43 Abs. 1 Nr. 3 BDSG.

4.1.2.3
Selbstauskunft

Die Betroffene nahm die unerwünschte Werbe-E-Mail zum Anlass, eine Selbstauskunft gem. § 34 Abs. 1 BDSG von dem Unternehmen zu verlangen.

§ 34 Abs. 1 BDSG

Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Der Geschäftsführer des Unternehmens reagierte zwar schnell, aber falsch, denn er benannte bei seiner Auskunft lediglich die Datenarten und nicht konkret die in seinem Unternehmen gespeicherten Daten der Kundin. Diese Art der fehlerhaften Auskunftserteilung geschieht leider immer noch sehr häufig, obwohl ich Unternehmen seit Jahren darauf hinweise, dass die gesetzlichen Anforderungen so nicht erfüllt werden (vgl. auch

41. Tätigkeitsbericht, Ziff. 4.7). Das Auskunftsrecht gehört nach § 6 Abs. 1 BDSG zu den unabdingbaren Rechten der Betroffenen. Nur wenn die Daten genau benannt werden, können weitere datenschutzrechtliche Schutzmechanismen, wie z. B. das Recht auf Berichtigung (§ 35 BDSG), greifen. Da die Wahrnehmung des Auskunftsrechts oftmals eine zentrale und wichtige Funktion für die Betroffenen hat, hat der Gesetzgeber in § 43 Abs. 1 Nr. 8a BDSG bei fehlender, unvollständiger, verspäteter oder falscher Auskunft verantwortlicher Stellen an Betroffene die Möglichkeit der Einleitung eines Ordnungswidrigkeitsverfahrens vorgesehen.

4.1.2.4
Betrieblicher Datenschutzbeauftragter

Der Empfehlung der datenschutzrechtlich sehr fachkundigen Betroffenen, zur Erteilung der Auskunft seinen betrieblichen Datenschutzbeauftragten hinzuzuziehen, entgegnete der Geschäftsführer, dass er keinen betrieblichen Datenschutzbeauftragten bestellt habe und diese Position aufgrund der (angeblichen) Wichtigkeit des Datenschutzes in seinem Unternehmen selbst einnehme.

Inhaber, Vorstände, Geschäftsführer und sonstige gesetzlich oder verfassungsmäßig berufene Vertreter einer verantwortlichen Stelle dürfen jedoch nicht die Position des betrieblichen Datenschutzbeauftragten einnehmen. Diese Inkompatibilität lässt sich bereits aus dem Wortlaut des § 4f Abs. 3 Satz 1 BDSG ableiten, wonach der Beauftragte für den Datenschutz dem Leiter der verantwortlichen Stelle unmittelbar zu unterstellen ist. Das entscheidende Argument gegen die Bestellung eines Mitglieds der Unternehmensleitung ist jedoch die Unzulässigkeit der Identität von Kontrollierendem und Kontrolliertem wegen der zwangsläufigen Interessenkonflikte. Die Nichtbestellung eines betrieblichen Datenschutzbeauftragten trotz offensichtlich vorliegender gesetzlicher Verpflichtung hierzu erfüllt den Bußgeldtatbestand des § 43 Abs. 1 Nr. 2 BDSG.

Das Unternehmen wurde nachdrücklich auf die Notwendigkeit einer Werbe-Einwilligung, des Widerspruchshinweises bei Werbung, eine korrekte Beauskunftung bei Selbstauskünften und die Erforderlichkeit der Bestellung eines betrieblichen Datenschutzbeauftragten hingewiesen und zeigte sich einsichtig: Eine betriebliche Datenschutzbeauftragte wurde umgehend bestellt, E-Mail-Werbung wird künftig vollständig unterlassen und Auskünfte nach § 34 Abs. 1 BDSG werden in Zukunft korrekt erteilt.

Aufgrund der Vielzahl der vorliegenden Verstöße wurde die Sache dennoch an die Bußgeldstelle meines Hauses zur Prüfung der Einleitung entsprechender Verfahren nach dem Gesetz über Ordnungswidrigkeiten weitergeleitet.

4.1.3
Bußgeldverfahren beim Einsatz sog. Dash-Cams im Straßenverkehr

Der Einsatz einer an der Windschutzscheibe eines Pkw installierten Videokamera, einer sog. Dash-Cam, ist weiterhin sehr beliebt und nur unter engen Voraussetzungen aus datenschutzrechtlicher Sicht zulässig. Oftmals zur Dokumentation von Unfällen oder verkehrsgefährdendem Verhalten anderer Verkehrsteilnehmer eingesetzt, kann die Benutzung dieser kleinen Videokamera ein Ordnungswidrigkeitenverfahren mit Erlass eines Bußgeldbescheids nach sich ziehen.

Dash-Cams sind Mini-Kameras, die in einem Kraftfahrzeug auf dem Armaturenbrett innen vor der Windschutzscheibe befestigt werden und den gesamten Straßenverkehr sowie das Randgeschehen aufzeichnen können. Sie erfreuen sich großer Beliebtheit bei den Autofahrern. Der Einsatz erfolgt unter anderem für Landschaftsaufnahmen, „Sightseeing“ in der Stadt oder aber auch zur Beweissicherung bei Gefährdungslagen und Unfällen oder der Dokumentation sonstigen strafbaren Verhaltens anderer Verkehrsteilnehmer.

4.1.3.1
Rechtlicher Rahmen von Videoaufzeichnungen im Straßenverkehr

Diese Videoaufzeichnungen durch Privatpersonen sind Datenerhebungen und daher ein Eingriff in das Recht auf informationelle Selbstbestimmung und unterliegen den Vorschriften des BDSG. § 6b BDSG regelt die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung).

§ 6b Abs. 1 und 3 BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

….

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

Meiner Meinung nach ist der Einsatz dieser Kameras im öffentlichen Straßenverkehr gemessen an § 6b BDSG grundsätzlich unzulässig. Dies habe ich bereits in meinem 42. Tätigkeitsbericht 2013 (Ziff. 4.2.2.6) festgestellt, entsprechend dem Beschluss der Aufsichtsbehörden über den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 25./26.02.2014). Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG ist danach eine Beobachtung und Aufzeichnung mittels Videokamera nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diese Voraussetzungen sind in aller Regel jedoch nicht erfüllt, da die schutzwürdigen Interessen der anderen Verkehrsteilnehmer überwiegen. Dash-Cams zeichnen den Verkehr ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Beweismittel in der Hand zu haben, kann den gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen.

4.1.3.2
Dash-Cam-Aufzeichnungen als Ordnungswidrigkeit

Wer entgegen § 6b BDSG den Straßenverkehr videoüberwacht, begeht eine Ordnungswidrigkeit gem. § 43 Abs. 2 Satz 1 BDSG, da unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhoben werden. Diese Ordnungswidrigkeit kann mit einer Geldbuße bis zu 300.000 EUR geahndet werden. Im Berichtsjahr 2015 wurden von mir erstmals mehrere Ordnungswidrigkeitenverfahren im Zusammenhang mit dem Einsatz sog. Dash-Cams im Straßenverkehr abgeschlossen.

In allen Fällen filmte ein Autofahrer das Verkehrsgeschehen mit einer Dash-Cam und händigte später der Polizei die Aufnahmen aus. Dokumentiert werden sollte jeweils das verkehrswidrige Verhalten anderer Verkehrsteilnehmer, die etwa andere Autos auf dem Standstreifen überholten, andere Verkehrsteilnehmer bedrängten oder durch Handzeichen beleidigten. Auch ein Unfall mit einem nur geringen Sachschaden wurde gefilmt.

4.1.3.2.1
Erhebung personenbeziehbarer Daten

Oftmals wurde in den einzelnen Verfahren eingewandt, man könne ja kaum eine Person erkennen bei den rasanten Aufnahmen während der Autofahrt und ein Kennzeichen müsse auch nicht gleich auf eine bestimmte Person schließen lassen, so dass fraglich sei, ob das BDSG überhaupt anzuwenden wäre. Diese Einschätzung ist jedoch falsch, da Kfz-Kennzeichen immer personenbeziehbar sind. Auch sind bei Aufnahmen von Personen diese immer erkennbar, da der Film etwa auch langsam abgespielt werden kann. Dies gilt auch für Passanten am Straßenrand, bei denen ebenfalls eine Datenerhebung stattfindet.

4.1.3.2.2
Die Videoaufnahme als Beweismittel gegen „Verkehrssünder“

Im Rahmen der Anhörung im Ordnungswidrigkeitenverfahren nach § 55 OWiG wurde von den Betroffenen oft hervorgebracht, dass man ja nur die „Verkehrssünden“ anderer beweisen und somit zur Aufklärung des Sachverhalts beitragen wollte. Im Übrigen seien in der letzten Zeit Urteile von Gerichten ergangen, die eine solche Videoaufnahme als Beweismittel akzeptiert hätten. Die jeweils genannten Urteile beschäftigten sich jedoch alle mit der Frage, ob die Dash-Cam-Aufzeichnungen im Einzelfall in ein Zivil- oder Strafverfahren als Beweis eingebracht werden konnten. Nicht beurteilt wurde die Frage der datenschutzrechtlichen Zulässigkeit. Nur hierauf kommt es aber an bei der Prüfung durch die Datenschutzaufsicht, ob der Tatbestand einer Ordnungswidrigkeit verwirklicht ist. Bei der Frage, ob etwa im Strafrecht ein Beweisverwertungsverbot vorliegt, werden ganz andere Voraussetzungen geprüft. Somit darf man sich nicht durch eventuell in der Presse herumgeisternde Meldungen irritieren lassen.

4.1.3.2.3
„Unwissenheit schützt vor Verhängung eines Bußgeldes nicht“

Auch das Argument, man wusste ja gar nicht, dass das Filmen mit einer Dash-Cam mit der Zahlung eines Bußgelds enden kann, verfängt nicht. Unwissenheit schützt auch hier vor Strafe bzw. der Verhängung eines Bußgelds nicht. Nach § 11 Abs. 2 OWiG handelt ein Täter dann nicht vorwerfbar, wenn er den Irrtum über das Bestehen oder die Anwendbarkeit einer Rechtsvorschrift nicht vermeiden konnte, ein sog. Verbotsirrtum. Es ist jedoch davon auszugehen, dass jedermann weiß, dass man nicht einfach ohne Einwilligung Foto- oder Filmaufnahmen von anderen fremden Personen anfertigen kann. Auch wenn diese Aufnahmen nur „im Vorbeifahren“ entstehen und einzelne Personen vielleicht verschwommen zu sehen sind, bleiben es Videoaufnahmen von Verkehrsteilnehmern, die auch durch das Kfz-Kennzeichen zu identifizieren sind. Es ist allgemein bekannt und entspricht dem Rechtsempfinden der Allgemeinheit, dass niemand Foto- und Videoaufnahmen von anderen Personen ohne deren Einwilligung machen darf, es sei denn, dies geschieht im privaten Rahmen. Selbst wenn dies einem Dash-Cam-Nutzer im Einzelfall nicht bewusst ist, so hat er bei der Anschaffung eines solchen technischen Geräts die Pflicht, sich zu erkundigen, in welchem rechtlichen Rahmen er es einsetzen kann. Allenfalls ist Unkenntnis zu berücksichtigen bei der Frage, ob vorsätzlich oder fahrlässig gehandelt wurde. Dies hat dann wiederum Auswirkungen auf die Höhe des zu verhängenden Bußgelds.

Die Höhe der Bußgelder bemisst sich jeweils an der wirtschaftlichen Situation der Betroffenen. Da auch kein wirtschaftlicher Vorteil durch die Datenerhebung erlangt werden sollte, wurden Bußgelder nur im unteren Bereich des Bußgeldrahmens verhängt. Mein Ziel war es in erster Linie, klarzustellen, dass das Filmen und Überwachen des öffentlichen Straßenverkehrs in „Hilfs-Sheriff-Manier“ nicht erlaubt ist.

4.2
Vereine

4.2.1
Erstellung von bundesweit einheitlichen Mitgliedspässen durch einen deutschen Sportverband über ein Internet-Portal

Werden personenbezogene Daten von einer verantwortlichen Stelle für einen bestimmten Zweck (Ausstellung von Mitgliedspässen) erhoben, sind die Daten zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

4.2.1.1
Ausgangslage

Ein deutscher Sportverband betreibt als verantwortliche Stelle gemäß § 3 Abs. 7 BDSG seit 2012 ein Internet-Portal, um vor allem den in dem Verband organisierten Vereinen ein besseres und leichteres Arbeiten mit den einzelnen Landesverbänden und dem Bundesverband zu ermöglichen.

§ 3 Abs. 7 BDSG

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

Konkret stehen unter anderem folgende Leistungen zur Verfügung:
– Online-Bestellung von individuellen Mitgliedspässen
– Online-Bestellung der neuen Wettkampflizenzen
– Eingabe und Abrufen von Veranstaltungsterminen
– individuelle Datenspeicherung
– verbesserte Kommunikation.

Derzeit sind von ca. 2500 Vereinen in der Bundesrepublik 2175 Vereine im Internet-Portal angemeldet und nutzen diesen Service.

Die zentrale Vergabe der Mitgliedspässe über das Internet-Portal sorgte in vielen Landesverbänden für Kritik, da bis 2012 die Mitgliedspässe als Blankopässe an die Vereine übersandt und vom jeweiligen Verein handschriftlich ausgestellt wurden.

Ein Grund für die zentrale Vergabe der Mitgliedspässe waren immer wieder auftretende Unregelmäßigkeiten bei der handschriftlichen Ausstellung der Pässe durch die Vereine. Hierbei konnte nicht ausgeschlossen werden, dass eine Person für verschiedene Vereine startete oder Mitglieder bei der Meldung zum Stichtag unterschlagen wurden, um weniger Beiträge an den Bundesverband abführen zu müssen.

Aktuell bat mich der Hessische Landesverband um Überprüfung der Rechtmäßigkeit der Datenübermittlungen von den Vereinen an den Bundesverband und um Klärung der Frage, wie lange die Mitgliederdaten vom Bundesverband gespeichert werden dürfen.

Für die Mitgliedspassbestellung werden von den Vereinen über ein Internet-Portal folgende Daten übermittelt:

– Name
– Vorname
– Geschlecht
– Staatsangehörigkeit
– Geburtstag
– Geburtsort
– Vereinseintritt
– Lichtbild.

Außerdem beinhaltet der Pass noch folgende Angaben:

– Name des Vereins
– Landesverband
– Ausstellungsdatum.

Nach Eingabe der Daten muss der zuständige Landesverband den Pass freigeben. Der Pass wird dann durch einen Dienstleister des Bundesverbandes gedruckt und von dem Dienstleister unmittelbar an den jeweiligen Verein versandt. Ein Vertrag nach § 11 BDSG zwischen dem Bundesverband und dem Dienstleister liegt vor.

§ 11 BDSG

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) 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.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

   die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Auf Anfrage der Aufsichtsbehörde teilte der Bundesverband mit, dass derzeit beim Bundesverband die Datensätze von ca. 46.502 Mitgliedern dauerhaft gespeichert werden und es kein Löschkonzept gibt. Auch bei Vereinsaustritt oder bei Tod eines Passinhabers werden dessen Daten durch den Bundesverband nur gelöscht, wenn der Betroffene oder die Hinterbliebenen dies verlangen.

Auf die Frage, zu welchem Zweck der Bundesverband die Datensätze der Mitgliedspässe dauerhaft speichert, teilte dieser mit, dass bei Verlust eines Passes die Daten gleich wieder greifbar wären. Eine Verknüpfung der gespeicherten Datensätze mit der Wettkampflizenz finde zwar derzeit nicht statt. Dies wäre jedoch eine Option für die Zukunft, hierzu gäbe es aber noch keine konkrete Planung. Eine Kollisionsprüfung durch den Bundesverband finde nicht statt, das sei Aufgabe der Landesverbände. Neben den antragstellenden Vereinen können auch die jeweils zuständigen Landesverbände auf die Datensätze zugreifen.

Die beim Bundesverband gespeicherten Datensätze werden nicht an Dritte weitergegeben.

Auf die Frage, ob und wie die Vereine für ihre Mitglieder transparent machen, dass die Datensätze der Mitgliedspässe beim Bundesverband dauerhaft gespeichert werden und eine Löschung nur erfolgt, wenn der Betroffene dies einfordert, konnte der Bundesverband keine eindeutige Antwort geben. Es ist daher davon auszugehen, dass dem größten Teil der Passinhaber nicht klar ist, dass der Bundesverband ihre Daten dauerhaft speichert und erst auf Zuruf löscht.

4.2.1.2
Datenschutzrechtliche Bewertung

Bereits Anfang 2013 hatte die Datenschutzaufsichtsbehörde in NRW offenbar aufgrund einer Anfrage des dortigen Landesverbandes in einer ausführlichen Bewertung der Sachlage festgestellt, dass es ein durchaus legitimes Anliegen eines Bundesverbandes sei, die Gestaltung und Ausstellung der Mitgliedspässe einheitlich zu regeln und zentral zu steuern. Die Übermittlung der Mitgliedsdaten für die Ausstellung der Mitgliedspässe von den Vereinen an den Bundesverband ist auf der Grundlage des § 28 Abs. 2 Nr. 2a BDSG zulässig.

§ 28 Abs. 2 Nr. 2a BDSG

Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig
1. ...
2. soweit es erforderlich ist,
   a) zur Wahrung berechtigter Interessen eines Dritten oder

...

Der Rechtsauffassung der nordrhein-westfälischen Aufsichtsbehörde schließe ich mich an, was die Zulässigkeit des Verfahrens und die Datenübermittlung betrifft.
Die Frage der Datenlöschung wurde 2012 nicht aufgeworfen. Hier ging man offenbar davon aus, dass der Bundesverband die Vorschriften des BDSG beachtet.

Nach § 35 Abs. 2 S. 2 Ziff. 3 BDSG sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist.

§ 35 Abs. 2 S. 2 Ziff. 3 BDSG

(2) ... 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

Nach dem Druck der Mitgliedspässe werden die personenbezogenen Daten der einzelnen Vereinsmitglieder beim Bundesverband nicht mehr benötigt. Der Zweck der Datenübermittlung, nämlich Druck eines einheitlichen Mitgliedspasses, ist erfüllt und daher ist die weitere Speicherung der Datensätze nicht mehr erforderlich und sie sind zu löschen.

Ich hatte den Bundesverband zur Stellungnahme in dieser Sache aufgefordert und noch einmal Gelegenheit gegeben, darzulegen, ob es hinsichtlich der Zweckbestimmung noch andere Erfordernisse gibt, die eine dauerhafte Speicherung der Datensätze der einzelnen Mitglieder durch den Bundesverband rechtfertigen.

Die vom Bundesverband dargestellten Argumente begründen hinsichtlich des Zwecks der Datenübermittlung und Datenerhebung – nämlich Druck eines einheitlichen Mitgliedspasses – nicht die dauerhafte Speicherung der Daten der Passinhaber durch den Bundesverband.

Ich habe daher den Bundesverband aufgefordert, alle bis heute gespeicherten personenbezogenen Daten von Passinhabern gemäß § 35 Abs. 1 S. 2 Ziff. 3 BDSG zu löschen und künftig dafür Sorge zu tragen, dass die Daten neuer Passinhaber nach der Erstellung des Mitgliedspasses wieder gelöscht werden.

Der Bundesverband hat mittlerweile versichert, dass er alle gespeicherten Datensätze gelöscht hat und künftig neu übermittelte Datensätze nach Erstellung und Versendung der Mitgliedspässe gelöscht werden.

4.3
Auskunfteien und Inkassounternehmen

4.3.1
Speicherdauer von Daten bei Auskunfteien

Auskunfteien wie die SCHUFA Holding AG dürfen Daten zum Zweck der Auskunftserteilung nicht zeitlich unbegrenzt speichern. Vielmehr gibt das BDSG vor, unter welchen Bedingungen die Daten wieder zu löschen sind. Da die Löschung von negativen Einträgen erhebliche Auswirkungen auf die Beurteilung der Bonität hat, ist für viele Betroffene die Frage nach dem Zeitpunkt der Löschung solcher Einträge entscheidend.

Immer wieder erreichen mich Beschwerden und Anfragen, die den Zeitpunkt der Löschung von bei der SCHUFA Holding AG gespeicherten Daten betreffen. In der Regel handelt es sich bei den Daten, deren Löschung begehrt wird, um sog. Negativeinträge (z. B. unbezahlte Forderungen), die Erteilung der Restschuldbefreiung oder um ehemalige Anschriften der Betroffenen. Negativeinträge und Einträge zu einem Insolvenzverfahren haben immer eine

negative Auswirkung auf die Bonitätsbeurteilung der Betroffenen. Die Anzahl der gespeicherten ehemaligen Anschriften eines Betroffenen kann zumindest unter bestimmten Umständen negative Auswirkungen auf die Bonitätsbeurteilung haben. Daher haben Betroffene mit Negativeinträgen oder vielen ehemaligen Anschriften häufig ein großes Interesse daran, dass die gespeicherten Daten so früh wie möglich aus ihrem Datensatz bei der SCHUFA Holding AG gelöscht werden.

Die Löschung von bei Auskunfteien gespeicherten Daten ist in § 35 Abs. 2 S. 2 Nr. 4 BDSG geregelt.

§ 35 Abs. 2 S. 2 Nr. 4 BDSG

Personenbezogene Daten sind zu löschen, wenn

…

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Die Norm verpflichtet die Auskunfteien nach Ablauf einer Frist dazu, zu überprüfen, ob die Speicherung der Daten weiterhin erforderlich ist oder nicht. Bis zu dieser Prüfung, also bis zum Ablauf der Frist, dürfen zulässig erhobene Daten stets gespeichert werden. Ergibt die Prüfung, dass die Speicherung nicht mehr erforderlich ist, sind die Daten zu löschen. Ist es jedoch ausnahmsweise erforderlich, die Daten weiterhin zu speichern, darf die Auskunftei dies tun und die Daten auch weiterhin auf berechtigte Anfragen an Dritte übermitteln.

Die Frist, nach deren Ablauf die Erforderlichkeit der weiteren Speicherung zu prüfen ist, beginnt mit dem Ende des Jahres, in dem das jeweilige Datum erstmalig gespeichert wurde. Zusammenhängende Sachverhalte, wie z. B. verschiedene Meldungen zu einer bestimmten Forderung (z. B. Entstehung, Salden, Erledigung), sind dabei einheitlich zu betrachten. So richtet sich beispielsweise die Prüfpflicht zur Löschung einer Forderungshistorie nach dem Zeitpunkt der erstmaligen Einmeldung der Forderung bei der Auskunftei.

Je nachdem, ob es sich bei der gespeicherten Information um einen noch fortdauernden oder einen erledigten Sachverhalt handelt, läuft die Frist bis zur Prüfung für vier bzw. drei Jahre. Erledigte Sachverhalte sind beispielsweise bereits bezahlte Forderungen, beendete

Insolvenzverfahren (und damit die erteilte Restschuldbefreiung) oder ehemalige Anschriften. Noch andauernde Sachverhalte sind z. B. laufende Kredite, bestehende Konten oder offene Forderungen.

Solange Sachverhalte andauern, ist die weitere Speicherung von Informationen darüber auch nach Ablauf der Prüfungsfrist in aller Regel erforderlich. Es ist gerade der Zweck von Wirtschaftsauskunfteien, Informationen über laufende Geschäfte eines Betroffenen zu speichern und zu übermitteln. Anhand aktueller Daten können zudem zutreffende Bonitätsbeurteilungen vorgenommen werden. Daher kann beispielsweise die Information, dass ein Kredit oder eine offene Forderung besteht, mindestens so lange gespeichert werden, bis dieser abbezahlt ist.

Auch Informationen über bereits erledigte Sachverhalte können für die Beurteilung der Bonität einer Person durchaus noch relevant sein, da aus dem Verhalten in der Vergangenheit Schlüsse auf zukünftiges Verhalten gezogen werden können. Die Aussagekraft solcher Daten schwindet jedoch mit der Zeit. Liegt die Erledigung bereits längere Zeit zurück, wird die Prüfung nach Ablauf der gesetzlichen Frist daher in der Regel ergeben, dass die weitere Speicherung des erledigten Sachverhalts nicht mehr erforderlich ist und dieser deshalb zu löschen ist. Bestimmte erledigende Ereignisse, die eine über die Erledigung der einzelnen Forderung hinausgehende Aussagekraft haben (z. B. die Erteilung der Restschuldbefreiung), sind grundsätzlich drei Jahre nach Ablauf des Jahres zu löschen, in dem sie eingetreten sind (s. a. 42. Tätigkeitsbericht, Ziff. 4.3.3).

Etwas anderes gilt für Anschriftendaten, die von Auskunfteien nicht nur für die Beurteilung der Bonität, sondern vor allem auch für die Identifizierung der Betroffenen genutzt werden (s. 43. Tätigkeitsbericht, Ziff. 5.3.10). Die Anschrift ist ein wesentliches Merkmal, anhand dessen Personen identifiziert werden. Da Anfragen und Meldungen bei Auskunfteien nur unregelmäßig eingehen, sich die Anschrift durch Umzüge aber verhältnismäßig häufig ändert, benötigen Auskunfteien oft auch noch ehemalige Anschriften, um Anfragen oder Meldungen der richtigen Person zuordnen zu können. Aus diesem Grund ist die Speicherung von ehemaligen (und damit „erledigten“) Anschriften eines Betroffenen regelmäßig auch über die gesetzliche Frist hinaus erforderlich. Allerdings ist nach Ablauf einer zweiten Prüfungsfrist (also sechs Jahre nach dem Ende des Jahres, in dem die Anschrift durch einen Umzug zur ehemaligen Anschrift wurde) die alte Anschrift derart veraltet, dass sie auch zu diesem Zweck nicht mehr erforderlich ist. Sie ist damit regelmäßig nach Ablauf von sechs Jahren seit dem Jahr des Umzugs zu löschen.

4.3.2
Prüfung von Auskunfteien

Im Berichtsjahr habe ich einige Auskunfteien geprüft und dabei lediglich in wenigen Fällen Beanstandung aussprechen müssen.

In meinem 43. Tätigkeitsbericht (Ziff. 5.3.9) hatte ich über die Unzulässigkeit der Beauskunftung von bestrittenen Daten, deren Richtigkeit durch die verantwortliche Stelle nicht nachgewiesen werden konnte, berichtet. Seinerzeit habe ich die verantwortliche Stelle mittels einer Anordnung dazu verpflichtet, in einem solchen Fall (Sperrung der Daten) gegenüber Dritten eine neutrale Auskunft zu erteilen und die Tatsache der Sperrung nicht mitzuteilen. Um die Umsetzung meiner Anordnung zu überprüfen, habe ich neben der betroffenen Auskunftei neun weitere vergleichbare Auskunfteien überprüft.

Festgehalten werden kann, dass die von mir gestellten Anforderungen bei allen zehn Unternehmen umgesetzt worden sind. In diesem Bereich gab es meinerseits keine Beanstandungen.

Unter den geprüften Unternehmen befanden sich auch solche, die neben der Auskunfteientätigkeit auch Inkassodienstleistungen anbieten. Insofern wurde überprüft, ob die Unternehmen eine Trennung zwischen den Beständen der Auskunfteiendaten und der Inkassodaten gewährleisten. Hierbei kam es ebenfalls zu keinerlei Beanstandungen.

Größtenteils unproblematisch erwiesen sich ferner die Prüfungsbereiche Auskunft über die zur Person gespeicherten Daten nach § 34 BDSG, Verpflichtung der Mitarbeiter auf das Datengeheimnis nach § 5 BDSG sowie die stichprobenartige Überprüfung des berechtigten Interesses bei Auskunftserteilung nach § 29 Abs. 2 Satz 5 BDSG.

§ 5 BDSG

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 29 Abs. 2 Satz 5 BDSG

Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

Versäumnisse konnten hingegen bei der Pflicht zur Benachrichtigung nach § 33 Abs. 1 Satz 2 BDSG festgestellt werden. Hiernach müssen die verantwortlichen Stellen die Betroffenen informieren, wenn erstmals Daten zu einer Person übermittelt werden, deren Speicherung ohne Kenntnis des Betroffenen erfolgt ist. Der Nachversand der entsprechenden Benachrichtigungen ist in allen Fällen zeitnah nachgeholt worden.

§ 33 Abs. 1 Satz 2 BDSG

Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

In einem Fall wurde festgestellt, dass kein betrieblicher Datenschutzbeauftragter bestellt worden war. Nach § 4f Abs. 1 Satz 6 BDSG muss ein Unternehmen, welches geschäftsmäßig Daten zum Zweck der Übermittlung erhebt (Auskunftei), einen Beauftragten für den Datenschutz bestellen. In diesem Fall habe ich ein Bußgeld verhängt.

§ 4f Abs. 1 Satz 6 BDSG

Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

4.3.3
Datenschutzrechtliche Einordnung von Adressauskunfteien

Auch Unternehmen, deren Auskunftstätigkeit sich auf die Überprüfung und Ermittlung von Anschriften beschränkt, haben die Regelungen des BDSG zu beachten, die für die gewerbliche Datenverarbeitung zum Zwecke der Übermittlung gelten. Das sind insbesondere die §§ 4d, 4f und 28 ff. BDSG.

Aufgrund von einigen Beschwerden bin ich auf Unternehmen aufmerksam geworden, die Adressüberprüfungen vornehmen. Dazu erhalten sie – meist von Inkassounternehmen – Einzeladressen oder Adresslisten, die dann auf Richtigkeit überprüft werden. Die Unternehmen überprüfen die gelieferten Adressen anhand ihres eigenen Datenbestandes oder durch individuelle Recherchen. Dabei werden auch Daten der Einwohnermeldeämter verarbeitet. Im Ergebnis werden veränderte Adresslisten oder neue Einzeladressen geliefert. Eine Bonitätsprüfung findet dabei nicht statt.

Gleichwohl werden dabei automatisiert und geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung im Sinne von § 4d Abs. 4 Nr. 1 BDSG verarbeitet. Für die grundsätzlich geltende Meldepflicht solcher Verfahren an die zuständige Aufsichtsbehörde gemäß § 4d Abs. 1 Satz 1 BDSG sind daher die Ausnahmevorschriften von § 4d Abs. 2 und 3 BDSG nicht anwendbar. Daher besteht für diese Verfahren die Meldepflicht gemäß § 4d Abs. 1 Satz 1 BDSG.

§ 4d BDSG

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle
1. zum Zweck der Übermittlung,
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

Zusätzlich haben solche Unternehmen unabhängig von der Anzahl der Beschäftigten einen Datenschutzbeauftragten zu bestellen, § 4f Abs. 1 Sätze 1, 4 und 6 BDSG.

§ 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. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

Schließlich dürfen die Adressdaten auch nur dann übermittelt werden, wenn vor der Übermittlung ein berechtigtes Interesse an der Übermittlung glaubhaft dargelegt wurde, § 29 Abs. 2 Nr. 1 BDSG.

§ 29 BDSG

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

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder
3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Die betroffenen Unternehmen waren zum Teil der Auffassung, dass auf sie die vorstehend genannten Regelungen nicht anwendbar seien. Mangels Erteilung von Bonitätsauskünften sei vor allem § 29 BDSG nicht anwendbar.

Die Vorschrift des § 29 BDSG ist jedoch auch auf gewerbliche Adressauskünfte anwendbar. Zwar erteilen Adressauskunftsunternehmen keine Bonitätsauskünfte wie klassische Auskunfteien. Dies ist aber für die Anwendung der Regelung von § 29 BDSG nicht erforderlich. Das BDSG definiert den Begriff der Auskunftei nicht. Der Begriff der Auskunftei wird in § 29 BDSG lediglich beispielhaft als ein Anwendungsfall der gewerblichen Datenverarbeitung zum Zwecke der Übermittlung aufgeführt. Das BDSG knüpft auch in den §§ 4d Abs. 4 und 4f Abs. 1 Satz 6 BDSG nur an die geschäftsmäßige Verarbeitung personenbezogener Daten zum Zwecke der Übermittlung an. Dies hat der Gesetzgeber auch

in § 29 BDSG so beibehalten und als Voraussetzung für dessen Anwendung ebenfalls nur das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung aufgestellt.

Unternehmen, die vor allem im Inkassoprozess Anschriften liefern, wirken außerdem in dem Arbeitsablauf des Inkassoprozesses mit. Geschehen hier Fehler, können Rechnungen an falsche Anschriften und – bei Personenverwechslungen durch eine fehlerhafte Anschriftenermittlung – auch an falsche Personen verschickt werden. In der Folge kann dies sogar dazu führen, dass Betroffene fälschlicherweise als zahlungsunfähig oder zahlungsunwillig an Auskunfteien gemeldet werden. Bei mehrmaligem unbemerktem Fehlversand kann bei einem Inkassounternehmen leicht der Eindruck entstehen, dass die Voraussetzungen für die Meldung des Betroffenen an eine Auskunftei gemäß § 28a Abs. 1 Nr. 4 oder 5 BDSG vorliegen. Die Tätigkeit dieser Unternehmen kann sich folglich auf die Bonität der Betroffenen maßgeblich auswirken.

§ 28a BDSG

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,
2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,
3. der Betroffene die Forderung ausdrücklich anerkannt hat,
4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
   b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,
   c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und
   d) der Betroffene die Forderung nicht bestritten hat oder
5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat.

Daher dürfen auch Unternehmen, die lediglich Adressauskünfte erteilen, diese nur nach der vorherigen Versicherung eines berechtigten Interesses erteilen. Zur Erleichterung der Arbeitsabläufe kann dies vereinfacht erfolgen. Besteht bei Beziehern von Adressen nur ein einziges mögliches Interesse, wie z. B. die Durchführung eines Inkassoverfahrens, reicht es aus, wenn dieses Interesse schriftlich vor Durchführung der Übermittlung versichert wird. Dies kann bereits in einem Vertrag zum Datenbezug entsprechend geregelt werden.

Das Gleiche gilt für die Übermittlung von Adresslisten. Hier kann für den Abruf oder die Übermittlung einer gesamten Liste ein berechtigtes Interesse dargelegt werden, wenn dies für die gesamte Liste identisch ist.

4.3.4
Untervertrieb von Auskunfteienleistungen

Auf Reseller von Auskunfteienleistungen sind die Regelungen des BDSG für Auskunfteien in vollem Umfang anzuwenden.

Aufgrund mehrerer Beschwerden wurde ich darauf aufmerksam, dass in Hessen verstärkt Unternehmen auftreten, die Leistungen anderer Auskunfteien im eigenen Namen und auf eigene Rechnung verkaufen. Häufig handelt es sich dabei um Auskünfte größerer und bereits etablierter Auskunfteien. Technisch ist der Kunde unmittelbar mit der Datenbank der Auskunftei verbunden, deren Auskünfte verkauft werden. Die Reseller haben keinen eigenen Einfluss auf den Inhalt der Auskünfte. Der Reseller hat daher auch keine Möglichkeit, die übermittelten Daten zu speichern oder zu verarbeiten.

Zusätzlich bin ich auf Unternehmen aufmerksam geworden, die aus mehreren Datenbanken bestehender Auskunfteien eine neue und damit umfassendere Leistung zusammenstellen. Auch bei diesen Resellern findet keine eigene Datenhaltung mehr statt.

Für Auskunfteien besteht die Pflicht, ihre Tätigkeit vor ihrer Inbetriebnahme gemäß § 4d Abs. 1 und 3 BDSG zu melden. Für Auskunfteien gelten die Ausnahmen von der Meldepflicht gemäß § 4d Abs. 2 und 3 BDSG nicht.

§ 4d BDSG

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle
1. zum Zweck der Übermittlung,
2. zum Zweck der anonymisierten Übermittlung oder
3. für Zwecke der Markt- oder Meinungsforschung

gespeichert werden.

Die Reseller von Auskunfteienleistungen betrachteten sich selbst nicht als Auskunfteien, sondern lediglich als Vertriebsunternehmen der Auskunftei, deren Auskünfte sie verkaufen. Sie waren deshalb auch nicht gemeldet.

Auch die Durchführung der für Auskunfteien obligatorischen Stichprobenkontrollen nach § 10 Abs. 4 Satz 3 BDSG war nicht sichergestellt.

§ 10 Abs. 4 BDSG

Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und

überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

Auf Nachfrage hatten die Unternehmen argumentiert, dass es sich bei ihnen mangels eigener geschäftsmäßiger Erhebung, Speicherung, Veränderung oder Nutzung personenbezogener Daten (§ 29 Abs. 1 BDSG) nicht um Auskunfteien handelt. Der Reseller ermögliche nur den Bezug von Auskünften einer anderen Auskunftei, welche die gesetzlichen Vorgaben einhalte.

§ 29 Abs. 1 BDSG

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

Eine Prüfung ergab jedoch, dass die vertraglichen Vereinbarungen zwischen dem Reseller und der Auskunftei darüber hinausgehen. Der Reseller verpflichtet sich vertraglich selbst zur Erbringung der Leistungen ohne dabei auf eine andere Auskunftei als Leistungserbringer zu verweisen. Daher mag er die Leistung unter Nutzung der Leistungen dieser Auskunftei erbringen. Rechtlich erbringt er die Leistung gegenüber seinem Kunden selbst. Insbesondere kommt kein Schuldverhältnis zwischen der die Daten liefernden Auskunftei und dem Kunden zustande. In einem zu prüfenden Fall hatte das Unternehmen sogar eine eigene Marke eingetragen und die Leistungen unter dieser Marke erbracht.

Aufgrund der rechtlichen Eigenständigkeit der erbrachten Leistungen und des entsprechenden Marktauftretens des Resellers betrachte ich den Reseller daher als Auskunftei. Ich konnte alle Unternehmen davon überzeugen, meiner Auffassung zu folgen. In einem Fall war aufgrund der bereits fortgeschrittenen Geschäftstätigkeit die Einleitung eines Ordnungswidrigkeitenverfahrens unumgänglich.

4.3.5
Im Berichtszeitraum noch kein gesetzlicher Änderungsbedarf zum Scoring der Handelsauskunfteien

Das Scoring wurde zum 01.04.2010 durch diverse Änderungen des BDSG neu geregelt. Die Auswirkungen dieser Änderungen wurden im Jahre 2014 durch ein Gutachten untersucht, welches für das Bundesministerium der Justiz und für Verbraucherschutz und das Bundesministerium des Innern erstellt wurde. Die Inhalte des Gutachtens wurden im Mai 2015 in dem Symposium „Scoring – Die Praxis der Auskunfteien, deutsches Datenschutzrecht und europäische Perspektiven“ diskutiert, in dem ich neben dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen die Auffassung der datenschutzrechtlichen Aufsichtsbehörden dargestellt habe.

Das Scoring wurde in § 28b BDSG vollständig neu geregelt.

§ 28b BDSG

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,
2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,
4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

Zum Scoring der SCHUFA Holding AG hatte ich bereits in meinem 43. Tätigkeitsbericht (Ziff. 5.3.8.1) umfangreich berichtet. In dem Symposium habe ich vor allem zu den Erfahrungen aus den Beschwerden über das Scoring der Handelsauskunfteien vorgetragen. Die bei mir eingegangenen Beschwerden betrafen vor allem Scorewerte, die nach Auffassung der Betroffenen deren Bonität nicht zutreffend beschrieben. Dafür konnten in den

meisten Fällen eine nicht ausreichende Datenbasis, die fehlende Berücksichtigung positiver Merkmale oder fehlerhafte Daten als Ursachen ermittelt werden.

Nach der Korrektur fehlerhafter Daten wurde aus den korrigierten Daten im Normalfall auch ein akzeptierter Scorewert ermittelt. Bei einer geringen Datenbasis oder bei der fehlenden Berücksichtigung positiver Merkmale war die Behandlung indes problematischer. In keinem Fall war jedoch das mathematisch-statistische Modell fragwürdig. Vielmehr waren die Daten nicht umfassend genug, um in dem jeweiligen Einzelfall der Beschwerdefälle einen belastbaren Scorewert zu ermitteln. Dennoch war aber in der weit überwiegenden Mehrzahl der Fälle auch mit wenigen Daten die Ermittlung eines belastbaren Scorewertes möglich.

Im Hinblick auf das Symposium ergab sich aus der Beschwerdepraxis, dass die in dem Gutachten vorgeschlagene stärkere Regulierung des Scorings nicht geeignet ist, die ermittelten Scorewerte belastbarer oder bei den Betroffenen akzeptierter zu machen. Eine Einschränkung der für das Scoring nutzbaren Daten führt jedenfalls dann, wenn davon statistisch erhebliche Merkmale betroffen sind, zu einer Verringerung der Qualität der ermittelten Scorewerte. Dies führt auch dazu, dass die Scorewerte durch die Betroffenen und durch die Bezieher der Scorewerte (Kreditinstitute und Handel) weniger akzeptiert werden.

Eine Grenze sollte allerdings bei Daten gezogen werden, bei denen Betroffene nach keinem Gesichtspunkt mit deren Verwendung im Scoring rechnen müssen und die ausschließlich für den privaten Bereich vorgesehen waren. Dies trifft vor allem auf Daten aus sozialen Netzwerken zu. Diese Daten sind weder statistisch ausreichend signifikant noch können sie beliebig durch Dritte genutzt werden. Daten mit einer sehr geringen Signifikanz sollten bei der Scorewertberechnung unberücksichtigt bleiben. Würden die vorstehend genannten Datenarten berücksichtigt, würde dies auch zu einer vollständigen Überwachung Betroffener ohne echten Nutzen führen. Dies wäre datenschutzrechtlich unvertretbar.

Eine über die derzeitigen Regelungen des BDSG hinausgehende Regulierung der verwendeten Scoringformeln halte ich dagegen nicht für zielführend. An deren Richtigkeit gab es im Verlauf meiner Prüfungen keinen ernsthaften Zweifel.

Allerdings wäre die Verbesserung der Transparenz für die Betroffenen sinnvoll. Zwar ist die Transparenz des Scorings im BDSG schon geregelt. Automatisch getroffene Einzelfallentscheidungen, die alleine auf Basis von Persönlichkeitsmerkmalen zum Nachteil des Betroffenen gefällt wurden, müssen diesem mitgeteilt werden, § 6a Abs. 2 Nr. 2 BDSG.

§ 6a BDSG

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

Der Anwendungsbereich von § 6a BDSG ist jedoch sehr eng. So ist bereits umstritten, ob die Nutzung eines Scorewertes unter § 6a BDSG fällt. Eine Transparenzpflicht besteht auch nur dann, wenn die Entscheidung alleine auf Basis von Persönlichkeitsmerkmalen getroffen wurde. Sind in der Entscheidung weitere Merkmale verwendet worden, kann die Anwendbarkeit zweifelhaft sein. Andere Merkmale könnten sich z. B. aus dem Wert einer Bestellung oder von bestellten Produkten ergeben. Werden auch diese Merkmale zur Entscheidungsfindung herangezogen, kann die Transparenzpflicht entfallen.

Auch die bereits geregelte Pflicht zur Offenlegung von ablehnenden Entscheidungen aufgrund von § 29 Abs. 7 BDSG ist nur bei Verbraucherdarlehensverträgen oder Verträgen über entgeltliche Finanzierungshilfen mit Verbrauchern anwendbar.

§ 29 Abs. 7 BDSG

Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im

Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

Zwar ist hierbei die Übermittlung eines Scorewertes nicht erforderlich. Jede Auskunft einer Auskunftei wäre für die Anwendung ausreichend. Immer häufiger werden aber auch Entscheidungen auf Basis eines Scorewertes getroffen, die keine Finanzierung zum Gegenstand haben. Dies hat zur Folge, dass automatisierte Einzelfallentscheidungen, die hauptsächlich auf Basis eines Scorewertes und außerhalb von Finanzierungen getroffen wurden, in der Regel intransparent bleiben. Betroffene wissen weder, dass ein Scorewert eine Entscheidung wesentlich beeinflusst hat, noch kennen sie den Lieferanten des Scorewertes. Ihnen ist in der Regel noch nicht einmal transparent, dass eine automatisierte Entscheidung getroffen wurde.

Bleibt die Entscheidung und der verwendete Scorewert aber intransparent, können Betroffene sich bei dem Lieferanten des Scorewertes auch nicht darüber informieren, ob die Datenbasis richtig war oder ob fehlerhafte Daten zu der ablehnenden Entscheidung geführt haben. Dies führt in der Folge dazu, dass fehlerhafte Daten auch nicht korrigiert werden.

Daher halte ich die Verbesserung der Transparenz für sinnvoll. Betroffene sollten bereits dann, wenn das Scoring eine ablehnende Entscheidung maßgeblich beeinflusst hat, über die Durchführung des Scorings informiert werden. Zusätzlich müssen Betroffene wissen, wer den maßgeblichen Scorewert geliefert hat. Nur dann können sie gemeinsam mit dem Lieferanten die Richtigkeit der Daten überprüfen.

Allerdings werden derzeit die Rahmenbedingungen für den Datenschutz durch die Datenschutz-Grundverordnung auf europäischer Ebene neu geordnet. Im Berichtszeitraum war es deshalb noch nicht sinnvoll, gesetzliche Änderungen zu veranlassen. Erst auf Basis des endgültigen Textes der Datenschutz-Grundverordnung können die Möglichkeiten der Schaffung von Transparenz sinnvoll diskutiert werden. Der abschließende Text lag jedoch im Berichtszeitraum noch nicht so rechtzeitig vor, dass der gesetzliche Änderungsbedarf ausreichend ermittelt werden konnte.

4.3.6
SCHUFA Holding AG

Die SCHUFA Holding AG (kurz: SCHUFA), die nach eigenen Angaben zu mehr als 66 Mio. Personen Daten speichert, bildete auch im aktuellen Berichtszeitraum wieder einen wesentlichen Schwerpunkt meiner Prüfungstätigkeit. Nach wie vor zählt der Bereich der Tätigkeit von Handelsauskunfteien zu den Bereichen, in denen die meisten Beschwerden eingehen.

4.3.6.1
Beschwerdeaufkommen

Bereits im Jahr 2014 hatte ich mich umfassend mit dem Verfahren der SCHUFA zur Erlangung einer Selbstauskunft nach § 34 BDSG befasst. Ich konnte erreichen, dass in vielen Fallgestaltungen die Anforderung von Personalausweiskopien durch die SCHUFA unterbleiben sollte. Dies wurde von der SCHUFA auch umgesetzt. Im aktuellen Berichtszeitraum sind daher die Beschwerden, in denen die Anforderung von Kopien eines Personalausweises gerügt wurde, sehr stark zurückgegangen. Dies trifft vor allem auf Fälle zu, in denen die Zusendung einer Selbstauskunft an die bei der SCHUFA als gegenwärtige Adresse gespeicherte Adresse verlangt wurde.

Viele der zur SCHUFA im Berichtszeitraum eingegangenen Beschwerden betrafen die Richtigkeit oder die fehlende Löschung von bei der SCHUFA gespeicherten Daten. In allen Beschwerdefällen wurde der Inhalt der Beschwerde auf datenschutzrechtlich fehlerhaftes Verhalten der SCHUFA überprüft. In vielen Fällen ergab sich bereits anhand des Beschwerdesachverhalts, dass die SCHUFA in Übereinstimmung mit dem Datenschutz gehandelt hatte. In diesen Fällen wurde den Beschwerdeführern die Sach- und Rechtslage umfassend erläutert.

Soweit die Beschwerde Anlass zur Anforderung einer Stellungnahme der SCHUFA bot, wurde diese angefordert und von der SCHUFA in aller Regel auch kurzfristig zur Verfügung gestellt. In keinem überprüften Beschwerdefall ergab sich ein der SCHUFA vorwerfbares Fehlverhalten. In einigen Fällen wurde jedoch fehlerhaftes Verhalten von Unternehmen festgestellt, die Daten zu Forderungen an die SCHUFA übermittelt hatten, obwohl die Voraussetzungen dafür nicht vorlagen. In diesen Fällen wurde das Beschwerdeverfahren gegen diese Unternehmen fortgeführt und ggf. an die zuständige Aufsichtsbehörde eines anderen Bundeslandes abgegeben. In allen Fällen wurden die Daten durch die SCHUFA korrigiert oder gelöscht, sofern dies notwendig war.

4.3.6.2
Auskunftspraxis im Onlinehandel

Im Onlinehandel ist es unzulässig, vor der Auswahl einer für den Onlinehändler risikobehafteten Zahlart eine Bonitätsauskunft einzuholen.

Aufgrund der Beschwerde des Kunden eines Onlinehändlers habe ich die Auskunftspraxis im Onlinehandel betrachtet. In dem Beschwerdefall wurde durch den Onlinehändler eine Bonitätsauskunft der SCHUFA zur Zahlartensteuerung eingeholt. Dabei wurde bereits vor der Darstellung möglicher Zahlarten (z. B. Rechnung oder Vorkasse) in dem Workflow des Onlineshops durch die Bonitätsauskunft geprüft, ob dem Kunden Zahlarten angeboten werden können, die für den Onlinehändler Risiken beinhalten. Als risikobehaftet werden Zahlarten betrachtet, die eine Vorleistung des Händlers erfordern. Dies ist insbesondere bei der Zahlart „Kauf auf Rechnung“ der Fall.

Im Beschwerdefall wurde erst nach der Einholung einer Bonitätsauskunft durch den Kunden im weiteren Verlauf des Workflows eine Zahlart ausgewählt, die für den Onlinehändler risikoarm ist. Die Bonitätsauskunft diente daher nur dazu, dem Kunden eine risikobehaftete Zahlungsoption anzubieten, die er offenbar ohnehin nicht auswählen wollte.

Für die Anforderung von Bonitätsauskünften muss ein berechtigtes Interesse vorliegen und gegenüber der Handelsauskunftei auch glaubhaft versichert werden (§ 29 Abs. 2 Nr. 1 BDSG).

§ 29 BDSG

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

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden.

§ 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn
1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Nach meiner Auffassung genügt das Interesse des Onlinehändlers an einer kundenfreundlichen Gestaltung des Workflows diesen Anforderungen nicht. Es wäre problemlos möglich, die Bonitätsabfrage erst dann durchzuführen, wenn eine risikobehaftete Zahlart ausgewählt wurde. Jedenfalls stehen der Bonitätsabfrage schutzwürdige Interessen des Kunden entgegen. Die Bonitätsauskunft enthält die gesamten Bonitätsdaten des Kunden, die beim Onlinehändler in vielen Fällen nicht benötigt werden. Zudem kann die Bonitätsauskunft das Scoring des Kunden und damit dessen Bonität negativ beeinflussen. Selbst dann, wenn vom Onlinehändler vor der Durchführung der Bonitätsabfrage eine Einwilligung des Kunden eingeholt wird, dürfte dem Kunden in der Regel nicht transparent sein, dass sich seine Einwilligung negativ auf seine Bonität auswirken könnte. Eine Einwilligung dürfte daher in den wenigsten Fällen wirksam sein.

Der SCHUFA konnte ich dennoch kein datenschutzwidriges Vorgehen vorwerfen. Auskunfteien wie die SCHUFA sind bei der Prüfung von Anfragen gemäß § 10 Abs. 4 Satz 1 und 2 BDSG privilegiert.

§ 10 Abs. 4 BDSG

Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht.

Entsprechende Vereinbarungen mit ihren Kunden vorausgesetzt, können sie zunächst die Zulässigkeit von Bonitätsabfragen unterstellen. Zwar gab die konkrete Beschwerde Anlass zur Prüfung im Sinne von § 10 Abs. 4 Satz 2 BDSG. Aus der einzelnen Abfrage ist jedoch nicht erkennbar, ob diese der kundenfreundlichen Gestaltung des Onlineshops ohne

konkrete Auswahl einer risikobehafteten Zahlart oder der Prüfung nach Wahl einer riskanten Zahlart dient. Die SCHUFA darf daher Anfragen in der Regel ungeprüft bedienen.

Betreiber von Onlineshops, die Bonitätsabfragen nur zur kundenfreundlichen Gestaltung ihres Workflows durchführen, müssen jedoch zukünftig mit aufsichtsrechtlichen Maßnahmen rechnen.

4.3.7
Vor-Ort-Prüfungen bei Inkassounternehmen

Im Berichtszeitraum wurden sowohl anlassbezogen als auch anlassunabhängig Vor-Ort-Prüfungen bei mehreren Inkassounternehmen durchgeführt.

Die analysierten Prozessabläufe wie etwa diejenigen
– der Übernahme des Mandats,
– des Telefoninkassos,
– der Identifikation Betroffener/Schuldner,
– der Auskunftserteilung
– der Zusammenarbeit mit Dritten (Rechtsanwälten, Auskunfteien, Dienstleistern)
entsprachen ganz überwiegend den datenschutzrechtlichen Bestimmungen und boten lediglich vereinzelt Anlass zur Kritik.

So konnten durch meine Hinweise weitere Verbesserungen bei der Auskunftserteilung (vgl. 43. Tätigkeitsbericht, Ziff. 5.3.11) oder des Umgangs mit Personalausweiskopien (Zulässigkeit der Anforderung nur im Ausnahmefall, Hinweis an die Betroffenen auf die Möglichkeit des Schwärzens nicht benötigter Daten bzw. des Passfotos) erreicht werden.

Im Ergebnis war den geprüften Unternehmen eine hohe Sensibilität hinsichtlich datenschutzrechtlicher Belange sowie in der Regel ein sehr gutes Datenschutzniveau zu attestieren.

4.4
Kredit- und Finanzwirtschaft, Spielbanken

4.4.1
Veröffentlichung von Interessentendaten im Exposé durch ein Finanzcenter

Auch das ungewollte Veröffentlichen von Bonitätsdaten stellt eine Übermittlung von Daten dar und kann mit einem Bußgeld geahndet werden.

Durch eine Eingabe wurde ich auf folgenden Sachverhalt aufmerksam gemacht: Die Betroffenen wollten eine Wohnung, vermittelt über ein örtliches Finanzcenter, anmieten. Zur Prüfung der Bonität vor Abschluss des Mietvertrags reichten sie dort Kopien der notwendigen Unterlagen ein (Personalausweis, Entgeltabrechnungen, ausgefüllten Interessentenbogen, Nachweis Haftpflichtversicherung). Diese Unterlagen wurden seitens des Finanzcenters fälschlicherweise zu dem Exposé des Objekts hochgeladen. In einem Zeitraum von etwas mehr als zwei Wochen konnten diese Daten somit von unberechtigten Dritten zur Kenntnis genommen werden. Insgesamt wurden in diesem Zeitraum fünfundvierzig Zugriffe auf das Exposé festgestellt. Dem Unternehmen selbst ist dies nicht aufgefallen. Erst durch die Mitteilung des Betroffenen wurde der Fehler bemerkt und die Entfernung der Daten vorgenommen.

Das Hochladen der Daten in das öffentlich abrufbare Exposé stellt, da auf das Exposé im vorgenannten Zeitraum zugegriffen worden ist, eine Übermittlung an Dritte dar. Aus diesem Grund in Verbindung mit den Kontodaten sowie einer unsicheren Prognose bezüglich der Verwendung der Daten durch Dritte waren in diesem Fall zusätzlich die Voraussetzungen für eine Meldepflicht nach § 42a BDSG gegeben. Dieser Pflicht zur Meldung an die Datenschutzaufsichtsbehörde ist das Unternehmen nicht nachgekommen, so dass die Einleitung eines Bußgeldverfahrens nach § 43 Abs. 2 Nr. 1 und Nr. 7 BDSG zurzeit geprüft wird.

§ 43 Abs. 2 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

…

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

4.4.2
Versand unverschlüsselter E-Mails durch Finanzunternehmen

Der Versand unverschlüsselter E-Mails durch Finanzunternehmen an ihre Kunden ist nur dann zulässig, wenn Maßnahmen zur Transportverschlüsselung (TLS/SSL) eingesetzt werden und die E-Mails keine Daten enthalten, welche eine bestehende Geschäftsbeziehung beschreiben. Bei Zugangsdaten, Kontonummern, Beträgen oder Zahlungsinformationen handelt es sich um Daten, die nicht per unverschlüsselter E-Mail übermittelt werden dürfen.

Im Berichtszeitraum erreichten mich mehrere Beschwerden über den Versand von unverschlüsselten E-Mails durch Finanzunternehmen. In einem Fall enthielt die E-Mail die umfassende Darstellung des Finanzstatus eines Kunden. In anderen Fällen waren vollständige Kontonummern, andere Nummern zur Identifikation des Kunden und/oder Kontostände enthalten.

In einem Fall war eine Kreditkartennummer enthalten, die durch das Ersetzen einiger Ziffern maskiert und damit unkenntlich gemacht wurde. Die maskierte Nummer war wegen der fehlenden Ziffern keinem konkreten Kunden mehr zuzuweisen. Die verantwortliche Stelle beabsichtigte den in der E-Mail genannten Betrag per SEPA-Lastschrift einzuziehen. Sie konnte sich daher darauf berufen, den Kreditkarteninhaber auf den bevorstehenden Lastschrifteinzug hinweisen zu müssen (SEPA-Lastschrift-Vorabinformation entsprechend den SEPA-Regularien).

Unverschlüsselt versandte E-Mails können grundsätzlich von Dritten mitgelesen werden. Insbesondere werden E-Mails auf den zum E-Mail-Versand verwendeten Servern gespeichert und können vom Betreiber des Servers gelesen werden. Dies gilt sowohl für den Server des Versenders und des Empfängers als auch für alle dazwischen zur Übermittlung ggf. verwendeten Server.

Bei den aus der Beziehung zum Kreditinstitut entstehenden Informationen handelt es sich im Falle von Privatkunden um personenbezogene Daten, weil die Daten einem Kontoinhaber zuzuordnen sind. Können die Daten auch ohne Kenntnis des Namens eines Kontoinhabers oder der Kontonummer einer natürlichen Person zugeordnet werden, bleiben die Daten auch dann personenbezogen, wenn der Name des Kontoinhabers oder die Kontonummer entfernt oder unkenntlich gemacht wird. Werden Finanzinformationen per E-Mail versendet, kann die E-Mail-Adresse ebenso einen Personenbezug herstellen wie eine Kontonummer oder der

Name des Kontoinhabers. Die Maskierung einer Kontonummer reicht im Falle des E-Mail-Versands daher nicht aus, um den Personenbezug der Daten aufzuheben.

Im Verhältnis des Kunden zu seinem Kreditinstitut gilt zusätzlich das Bankgeheimnis. Daraus ergibt sich sowohl die Verpflichtung zur vertraulichen Behandlung des Inhalts der Geschäftsbeziehung als auch des Umstandes, dass überhaupt eine solche Geschäftsbeziehung zwischen Kreditinstitut und Kunde besteht. Da Kreditkarten in der Regel von Kreditinstituten herausgegeben werden, unterliegen auch die im Kreditkartenverhältnis entstehenden Informationen dem Bankgeheimnis. Daran ändert auch die Pflicht zur SEPA-Lastschrift-Vorabinformation nichts.

Außerdem sind Daten nach § 9 BDSG und der dazu geltenden Anlage, dort insbesondere nach Nr. 4 (Weitergabekontrolle), beim Transport vor unbefugtem Zugriff zu schützen.

§ 9 BDSG

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

Anlage zu § 9 Satz 1

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,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

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),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Der unverschlüsselte Versand von E-Mails erfüllt diese Anforderungen nicht. Der Versand ist daher unzulässig, weil keine ausreichende Weitergabekontrolle (Anlage zu § 9 Satz 1 BDSG, Nr. 4) stattfindet. Auch die Notwendigkeit des Versands der Daten zur Vorbereitung des SEPA-Lastschrifteinzugs durch die SEPA-Lastschrift-Vorabinformation rechtfertigt den Versand nicht.

Zu berücksichtigen ist zusätzlich, dass sich aus einer E-Mail-Adresse häufig auf den Nutzer schließen lässt. Bei einer Verwendung der E-Mail-Adresse in sozialen Netzwerken lässt sich diese Verbindung auch leicht und ohne besondere Kenntnisse durch eine Internetrecherche nachvollziehen. Jedoch werden E-Mails mittlerweile in aller Regel mit einer Transportverschlüsselung (TLS/SSL) versendet. Dadurch wird zumindest der Zugriff während der Übermittlung erschwert.

Deshalb erscheint es nicht erforderlich, den Versand unverschlüsselter E-Mails generell zu untersagen. Insbesondere müssen Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen (§ 9 Satz 2 BDSG). Beim Versand sind Verfahren zur Transportverschlüsselung (TLS/SS) zu nutzen und die per E-Mail versendeten Daten sind auf ein Minimum zu beschränken. Unmaskierte Konto- und Kundennummern, Geldbeträge, Namen und personifizierte Anreden dürfen in solchen E-Mails nicht enthalten sein.

Die E-Mail eines Finanzdienstleisters an eine E-Mail-Adresse enthält dennoch mindestens die Information, dass zwischen dem Sender und dem Empfänger ein Kontakt besteht. Es muss sich jedoch nicht zwingend um das Bestehen einer Geschäftsbeziehung handeln. Vielmehr stellt dies nur ein Indiz für eine bestehende Geschäftsbeziehung dar. Eine E-Mail könnte auch zu Werbezwecken versandt worden sein. Der Umstand, dass überhaupt eine E-Mail vom Sender an den Empfänger versandt wurde, muss daher nicht zwingend geschützt werden.

Aus dem Inhalt ließe sich jedoch auf den Inhalt des Kontaktes und damit auf das Bestehen einer Geschäftsbeziehung schließen. Enthält die E-Mail aber über das Bestehen der Geschäftsbeziehung hinaus keine Inhalte, welche die Geschäftsbeziehung beschreiben (z. B. Zugangsdaten, Kontonummern, Beträge oder Zahlungsinformationen), erscheint eine Transportverschlüsselung mit TLS/SSL als ausreichende Maßnahme im Sinne von § 9 Satz 2 BDSG. Weitere Inhalte, insbesondere Inhalte, die den Zugang zu weiteren Informationen ermöglichen, dürften jedoch trotz Transportverschlüsselung in einer E-Mail nicht enthalten sein.

4.4.3
Datenübermittlung in die USA nach dem FATCA-Abkommen

Kreditinstitute sind nach der FATCA-USA-Umsetzungsverordnung dazu verpflichtet, die Kundenbeziehung auf eine mögliche US-Steuerpflicht zu überprüfen. Sofern eine US-Steuerpflicht angenommen wird, dürfen diese Daten über das Bundeszentralamt für Steuern an die Bundessteuerbehörde der Vereinigten Staaten von Amerika übermittelt werden.

Im Berichtszeitraum führten mehrere Betroffene Beschwerde darüber, dass ihnen von ihren Finanzinstituten Fragebogen zur Feststellung der US-Steuerpflicht mit einer festgesetzten Rückgabefrist zugesandt worden waren. Mit diesen Schreiben wurde darauf hingewiesen, dass die entsprechenden Daten über das Bundeszentralamt für Steuern an die US-

Steuerbehörde übermittelt würden, sofern eine Rückantwort durch die Kunden unterbleiben würde. Diese Praxis führte bei mir zu einigen Eingaben.

Nach § 4 Abs. 1 BDSG ist eine Datenübermittlung u. a. dann zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet.

§ 4 Abs. 1 BDSG

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

Als Rechtsgrundlage kam hier das „Abkommen zwischen der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten und hinsichtlich der als Gesetz über die Steuerehrlichkeit bezüglich Auslandskonten bekannten US-amerikanischen Informations- und Meldebestimmungen (FATCA-Abkommen)“ in Betracht, welches am 31.05.2013 unterzeichnet wurde. Das Zustimmungsgesetz zum Abkommen ist am 16.10.2013 (BGBl. II S. 1362) in Kraft getreten. Das FATCA-Abkommen wurde am 11.12.2013 wirksam.

Mit Ermächtigung des § 117c Abgabenordnung (AO) wurde die FATCA-USA-Umsetzungsverordnung (FATCA-USA-UmsV) erlassen, die am 23.07.2014 veröffentlicht wurde (BGBl. I S. 1222).

Hiernach sind Finanzinstitute dazu verpflichtet, geeignete Verfahren anzuwenden, um bei ihnen geführte Konten als US-amerikanische meldepflichtige Konten i. S. v. § 2 Abs. 4 der FATCA-USA-Umsetzungsverordnung (FATCA-USA-UmsV) zu identifizieren.

Bei der Prüfung wird in erster Linie zwischen Konten, die zum 30.06.2014 bereits bestanden haben, und Konten, die nach dem 30.06.2014 eröffnet wurden, unterschieden.

Bei Konten, die zum 30.06.2014 bereits bestanden, war durch die Finanzinstitute zu prüfen, ob der Saldo oder Wert der bestehenden Konten zum Stichtag 31.12.2014 mehr als 50.000 US-Dollar (250.000 US-Dollar bei rückkaufsfähigen Versicherungs- oder Rentenversicherungsverträgen) betrug. Unterhalb dieser Betragsgrenze war eine Meldepflicht nicht gegeben. Lag der Betrag oberhalb dieser Grenze, ist zusätzlich eine Indiziensuche in den bei dem Unternehmen gespeicherten Datensätzen angezeigt.

Anlage 1 Abschnitt II B Nr. 1 FATCA-Abkommen

1. Suche in elektronischen Datensätzen. Das meldende deutsche Finanzinstitut muss seine elektronisch durchsuchbaren Daten auf folgende US-Indizien überprüfen:
   a) Identifizierung des Kontoinhabers als Staatsbürger der Vereinigten Staaten oder eine in den Vereinigten Staaten ansässige Person,
   b) eindeutige Angabe eines Geburtsorts in den Vereinigten Staaten,
   c) aktuelle Post- oder Hausanschrift (einschließlich einer Postfach- oder c/o-Anschrift) in den Vereinigten Staaten,
   d) aktuelle Telefonnummer in den Vereinigten Staaten,
   e) Dauerauftrag für Überweisungen auf ein in den Vereinigten Staaten geführtes Konto,
   f) aktuell gültige, an eine Person mit Anschrift in den Vereinigten Staaten erteilte Vollmacht oder Zeichnungsberechtigung oder
   g) eine c/o- oder postlagernde Anschrift als einzige Anschrift des Kontoinhabers in den Unterlagen des meldenden deutschen Finanzinstituts. Im Fall eines bestehenden Kontos einer natürlichen Person, bei dem es sich um ein Konto von geringerem Wert handelt, gilt eine c/o-Anschrift außerhalb der Vereinigten Staaten nicht als US-Indiz.

Sofern der Datensatz ein oder mehrere dieser US-Indizien aufweist, darf das Finanzinstitut das Konto als US-amerikanisches meldepflichtiges Konto betrachten. Es kann allerdings auch eine Selbstauskunft verlangen, um Sicherheit über das Vorliegen der US-Steuerpflicht zu erlangen (Anlage 1, Abschnitt II B Nr. 4a (1) FATCA-Abkommen).

Bei Konten mit einem Wert von unter 50.000 US-Dollar zum 31.12.2014, die nach dem 30.06.2014 eröffnet worden sind, muss das Finanzinstitut eine Prüfung auf eine etwaige US-Steuerpflicht nicht vornehmen (Anlage 1, Abschnitt III A FATCA-Abkommen).

Bei Konten, deren Wert die vorgenannte Grenze übersteigt, muss sich das Finanzinstitut eine Selbstauskunft innerhalb von 90 Tagen nach Ablauf des Kalenderjahres, ab dem das Konto nicht mehr unter Unterabschnitt A fällt, beschaffen (Anlage 1, Abschnitt III B FATCA-Abkommen).

Insofern war die Zusendung der Fragebogen in den mir vorgelegten Fällen nicht zu beanstanden. Kern der Beschwerden war allerdings die Aussage der Finanzinstitute, bei nicht fristgerechter Rücksendung der Fragebogen eine Übermittlung der Daten vorzunehmen.

Auch dieses Vorgehen ist nicht zu beanstanden gewesen. Nach Abschnitt III Unterabschnitt D Satz 2 der Anlage 1 zum FATCA-Abkommen muss das Finanzinstitut für den Fall, dass es eine Selbstauskunft nicht erhält, das Konto als US-amerikanisches meldepflichtiges Konto betrachten.

Anlage 1 Abschnitt III D Satz 2 FATCA-Abkommen

Ist das meldende deutsche Finanzinstitut nicht in der Lage, eine gültige Selbstauskunft zu beschaffen, so muss es das Konto als US-amerikanisches meldepflichtiges Konto betrachten.

Insofern waren sowohl die Erhebung der Daten über den Fragebogen als auch die Übermittlung der Daten an das Bundeszentralamt für Steuern in den mir vorgelegten Fällen nicht zu beanstanden.

4.4.4
Digitales Haushaltsbuch

Die aktuell von verschiedenen Kreditinstituten in Hessen angebotene Nutzung von Cloud-basierten Haushaltsbüchern wurde stichpunktartig überprüft und die derzeitigen Konzepte wurden als datenschutzrechtlich zulässig beurteilt.

Einige Kreditinstitute bieten ihren Kunden inzwischen die kostenlose Nutzung von Cloud-basierten Haushaltsbüchern an. Mittels einer Webanwendung können Kunden ihre Zahlungen verwalten, Kategorien zuweisen, Budgets bilden, Kosten analysieren und Reports erzeugen. Dadurch können sich Nutzer relativ einfach einen Überblick über ihr Konsum- und Zahlungsverhalten verschaffen.

Ich habe mir daher verschiedene Haushaltsbücher diverser Banken und Sparkassen vorstellen lassen. Andere Kreditinstitute befinden sich mit ähnlichen Lösungen in den Startlöchern. Dabei wurde deutlich, dass Kreditinstitute mit dem Angebot zumindest derzeit noch unterschiedliche Ziele verfolgen. Während bei einigen die Kundenbindung und Kundengewinnung im Vordergrund steht, sind andere stark an den Kunden- und Zahlungsstromdaten sowie deren Auswertung interessiert. Die Nutzung der in einem Haushaltsbuch gespeicherten Daten aus dem Zahlungsverkehr findet in den §§ 28 ff. BDSG

keine Rechtsgrundlage, da die Nutzung der Daten durch das Institut weder für das Angebot „Haushaltsbuch“ notwendig ist noch für die Durchführung des Zahlungsverkehrs. Daher ist für die Nutzung der Daten durch das Institut eine Einwilligung im Sinne des § 4a Abs. 1 BDSG erforderlich, die den Umfang der Nutzung begrenzt. Aus deren inhaltlicher Gestaltung wird gleichzeitig auch die strategische Zielrichtung des Verwenders deutlich.

Je nach strategischer Zielrichtung fällt auch die in der Einwilligungserklärung enthaltene Information des Betroffenen über den Zweck und Umfang der Datenverarbeitung unterschiedlich umfangreich aus. Einige Kreditinstitute betrachten Haushaltsbücher derzeit lediglich als Kundenbindungsinstrument. Die Einwilligung umfasst daher kein eigenes Recht des Kreditinstitutes zur Nutzung der Daten. Bei anderen Kreditinstituten variieren die Datenverarbeitungszwecke von der Nutzung der Umsätze zur Erstellung von individuellen Angeboten bis zur umfassenden Kundenanalyse. Den meisten Einwilligungserklärungen gemein ist die Einwilligung in eine Zahlungsstromanalyse, die je nach Gestaltung einen unterschiedlichen Umfang einnimmt. Keine Berücksichtigung findet bislang die Budgetanalyse im Verhältnis zu Peergroups, die Risikoanalyse anhand einer Kosten- und/oder Budgetanalyse, die persönliche Analyse anhand der Konsumfrequenz, die Konsumrichtung, die Verteilung des Konsums auf die Tageszeit oder die Auswertung von Kontakten zu Konkurrenten. All dies ist aus den Daten jedoch problemlos auszuwerten.

Je umfangreicher ein Kreditinstitut die Kundendaten auswerten möchte, umso umfangreicher ist auch in einer Einwilligung auf diesen Zweck hinzuweisen. Die Anforderungen an eine Einwilligung sind in § 4a BDSG beschrieben.

§ 4a Abs. 1 und 3 BDSG

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.
…
(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

Zusätzlich sind Einwilligungen an den für Allgemeine Geschäftsbedingungen geltenden Maßstäben zu messen. Diese ergeben sich aus den §§ 305 ff. BGB. Dabei sind insbesondere die Anforderungen der §§ 305c Abs. 1 und 307 BGB zu beachten.

§ 305c Abs. 1 BGB

Bestimmungen in Allgemeinen Geschäftsbedingungen, die nach den Umständen, insbesondere nach dem äußeren Erscheinungsbild des Vertrags, so ungewöhnlich sind, dass der Vertragspartner des Verwenders mit ihnen nicht zu rechnen braucht, werden nicht Vertragsbestandteil.

§ 307 BGB

(1) Bestimmungen in Allgemeinen Geschäftsbedingungen sind unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist.

(2) Eine unangemessene Benachteiligung ist im Zweifel anzunehmen, wenn eine Bestimmung

1. mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist oder
2. wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist.

(3) Die Absätze 1 und 2 sowie die §§ 308 und 309 gelten nur für Bestimmungen in Allgemeinen Geschäftsbedingungen, durch die von Rechtsvorschriften abweichende oder diese ergänzende Regelungen vereinbart werden. Andere Bestimmungen können nach Absatz 1 Satz 2 in Verbindung mit Absatz 1 Satz 1 unwirksam sein.

In dem auf besondere Vertraulichkeit ausgerichteten Bankverhältnis wird eine umfassende Datenauswertung des Kreditinstitutes durch den Kunden nicht erwartet. Dieser erwartet allenfalls eine Auswertung der Umsätze nach Betrag und Häufigkeit sowie des Kontostandes. Anhand dieser Daten ermittelte Angebote aus dem Finanzsektor werden

sicher den üblichen Bankkunden nicht überraschen. Reaktionen eines Kreditinstitutes wegen eines ungewöhnlichen Konsumverhaltens, z. B. das Verlangen zusätzlicher Sicherheiten, dürften einen durchschnittlichen Bankkunden aber überraschen.

Darüber hinaus entfernt sich ein Kreditinstitut mit einer derart weiten Datenauswertung so weit vom gesetzlichen Grundgedanken nicht nur des BDSG, sondern auch der Geschäftsbeziehung zwischen Kreditinstitut und Kunde, dass eine Wirksamkeit der Einwilligung auch nach § 307 Abs. 1 BGB nicht mehr gegeben sein dürfte.

Zusätzlich ist zu berücksichtigen, dass der Kontoinhaber den Zahlungsstrom nur in geringem Maße kontrollieren kann. Zahlungen finden statt, ohne dass der Bankkunde diese beeinflussen kann, wenn er die gegen ihn gerichteten pekuniären Ansprüche erfüllen möchte. In vielen Fällen ist selbst eine Barzahlung (Onlinehandel, Konzertkarten) nicht mehr möglich.

Eine extensive Einwilligung zur Datennutzung im Bankverhältnis beeinträchtigt den Kunden daher in ganz besonderem Maße in seiner Privatsphäre und könnte diese vollständig aufheben. Deshalb halte ich Einwilligungen nicht in unbegrenztem Umfang für zulässig. Die Kreditinstitute, deren Einwilligungen zur Prüfung vorlagen, waren im Rahmen ihrer eigenen datenschutzrechtlichen Prüfungen zu dem gleichen Ergebnis gelangt.

Daher waren die mir vorgelegten Einwilligungserklärungen und die zum Zeitpunkt der Prüfung praktizierten Datenverarbeitungsvorgänge datenschutzrechtlich nicht zu beanstanden.

4.4.5
Videoidentifizierung

Bei der Videoidentifizierung durch Banken nach dem Geldwäschegesetz sind datenschutzrechtliche Anforderungen zu beachten, die nicht von allen im Markt verfügbaren Produkten standardmäßig unterstützt werden. Die Nutzung des Dienstes Skype ist unzulässig.

Ich wurde von einer in Frankfurt ansässigen Direktbank bei der Einführung eines Dienstes zur Fernidentifizierung mittels Videotelefonie um Rat gebeten. Kreditinstitute haben ihre Kunden vor Aufnahme einer Geschäftsbeziehung anhand von Ausweispapieren zu

identifizieren und die Identifizierung zu dokumentieren. Dazu ist bei der Kontoeröffnung in der Regel die Vorlage des Personalausweises erforderlich.

§ 3 Abs. 1 Nr. 1 GwG

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

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

…

§ 4 GwG

(1) Verpflichtete haben Vertragspartner und soweit vorhanden wirtschaftlich Berechtigte bereits vor Begründung der Geschäftsbeziehung oder Durchführung der Transaktion zu identifizieren. Die Identifizierung kann noch während der Begründung der Geschäftsbeziehung abgeschlossen werden, wenn dies erforderlich ist, um den normalen Geschäftsablauf nicht zu unterbrechen, und ein geringes Risiko der Geldwäsche oder der Terrorismusfinanzierung besteht.

(2) Von einer Identifizierung kann abgesehen werden, wenn der Verpflichtete den zu Identifizierenden bereits bei früherer Gelegenheit identifiziert und die dabei erhobenen Angaben aufgezeichnet hat, es sei denn, der Verpflichtete muss auf Grund der äußeren Umstände Zweifel hegen, dass die bei der früheren Identifizierung erhobenen Angaben weiterhin zutreffend sind.

(3) Zur Feststellung der Identität des Vertragspartners hat der Verpflichtete folgende Angaben zu erheben:

1. bei einer natürlichen Person: Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift,
2. bei einer juristischen Person oder einer Personengesellschaft: Firma, Name oder Bezeichnung, Rechtsform, Registernummer, soweit vorhanden, Anschrift des Sitzes oder der Hauptniederlassung und Namen der Mitglieder des Vertretungsorgans oder der gesetzlichen Vertreter; ist ein Mitglied des Vertretungsorgans oder der gesetzliche Vertreter eine juristische Person, so sind deren Firma, Name oder Bezeichnung,

Rechtsform, Registernummer, soweit vorhanden, und Anschrift des Sitzes oder der Hauptniederlassung zu erheben.

(4) Zur Überprüfung der Identität des Vertragspartners hat sich der Verpflichtete anhand der nachfolgenden Dokumente zu vergewissern, dass die nach Absatz 3 erhobenen Angaben zutreffend sind, soweit sie in den Dokumenten enthalten sind:

1. bei natürlichen Personen vorbehaltlich der Regelung in § 6 Abs. 2 Nr. 2 anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, insbesondere anhand eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes, ...

Die Vorlage von Ausweispapieren zur Durchführung der Identifizierung erfordert entweder das persönliche Erscheinen in den Räumen der Bank oder die Nutzung von Dienstleistungen zur Identifikation, die ebenfalls eine persönliche Anwesenheit des Kunden erfordern. Direktbanken, deren Geschäft häufig über das Internet abgewickelt wird, empfinden die fehlende Möglichkeit zur Identifikation mittels Internet häufig als Medienbruch und Behinderung ihrer Geschäftstätigkeit.

Um eine Identifizierung mittels Videoidentifikation und damit die Identifikation über das Internet zu ermöglichen, wurde von der für die Bankenaufsicht zuständigen Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ein Rundschreiben veröffentlicht. Dieses beschreibt die bankaufsichtsrechtlichen Anforderungen an die Identifikation unter Nutzung der Videotelefonie (BaFin-Rundschreiben 1/2014 vom 05.03.2014, Abschnitt III). Die datenschutzrechtlichen Anforderungen an die Nutzung der Videotelefonie sind in dem Rundschreiben jedoch nicht enthalten, weshalb ich von der Direktbank um Beratung gebeten wurde.

Die datenschutzrechtlichen Aufsichtsbehörden haben ihrerseits die Videotelefonie im Rahmen des Identifizierungsprozesses betrachtet. Daraus ergaben sich zusätzliche datenschutzrechtliche Anforderungen.

Datenschutzrechtliche Bedenken bestehen insbesondere gegen die Nutzung des Dienstes Skype, die Erstellung von Screenshots von Ausweispapieren ohne die Möglichkeit der Schwärzung von nicht benötigten Angaben, eine vollständige Audioaufzeichnung des Identifizierungsvorgangs und die fehlende Transparenz der Löschungspflicht bzgl. der aufgezeichneten Daten bei Abbruch des Identifizierungsvorgangs.

Der Dienst Skype wird als nicht hinreichend sicher betrachtet. Die Nutzungsbedingungen sehen vor, dass Nutzer anderen Nutzern sehr umfassende Rechte an den versendeten Inhalten einräumen. Dies ist bei Kopien von Personalausweisen nicht möglich. Darüber hinaus lassen die – häufig wechselnden – Nutzungsbedingungen von Skype in einigen Fassungen eine Nutzung der aufgezeichneten Inhalte durch die Microsoft Corporation zu. Nicht zuletzt erfolgt eine Übertragung der Daten in Länder, deren Datenschutzniveau aus europäischer Sicht als nicht ausreichend betrachtet wird. Dabei ist zu berücksichtigen, dass bei der Identifikation alle Identifikationsdaten und dabei auch elektronische Kopien von Ausweispapieren übermittelt werden. Die Nutzung von Skype zur Identifikation ist daher unzulässig. Kreditinstitute, die eine Nutzung von Skype im Rahmen der Identifikation anbieten, müssen mit aufsichtsrechtlichen Maßnahmen rechnen.

Auch die vollständige Audioaufzeichnung des Identifizierungsvorgangs ist nicht erforderlich und verstößt daher gegen das Prinzip der Datensparsamkeit. Außerdem sind Möglichkeiten zu schaffen, welche die Schwärzung nicht benötigter Angaben auf Ausweispapieren ermöglichen. Das sind z. B. die Angaben zur Körpergröße und der Augenfarbe.

Der Direktbank wurden die datenschutzrechtlichen Anforderungen umfassend erläutert. Aufgrund meiner Beratung wurde die Videotelefonie mit reduziertem Funktionsumfang eingeführt. Dadurch können nicht nur die datenschutzrechtlichen Anforderungen erfüllt werden. Zusätzlich wurde auch der Aufwand zur Speicherung reduziert.

4.4.6
Whistleblowing-Richtlinie bei einem Kreditinstitut

Interne Regelungen, die Mitarbeiter zur Meldung von Gesetzesverstößen verpflichten (Whistleblowing-Richtlinien), müssen diese Verpflichtung konkret und leicht nachvollziehbar beschreiben. Sie müssen nicht nur den Mitarbeiter schützen, dem ein Gesetzesverstoß vorgeworfen wird, sondern auch den Mitarbeiter, der zur Meldung verpflichtet wird und dieser Verpflichtung nachkommt.

Durch eine Presseveröffentlichung wurde ich auf die interne Whistleblowing-Richtlinie eines Kreditinstitutes mit Sitz in Frankfurt am Main aufmerksam. Amerikanische Gesetze verpflichten Unternehmen, deren Wertpapiere in den USA gehandelt werden, zur Beachtung zahlreicher Anforderungen an die Richtigkeit der Finanzberichterstattung. Dazu zählen auch

Vorschriften zur Beachtung aller gesetzlichen Regelungen, der Compliance und zur Schaffung von Hinweisgebersystemen, um Gesetzesverstöße erkennen und beseitigen zu können. Deshalb verpflichten Unternehmen ihre Mitarbeiter häufig zur Meldung von Gesetzesverstößen in Whistleblowing-Regelungen.

Werden solche Meldungen erstattet, führt dies zur Verarbeitung der Daten des Meldenden und des Beschuldigten. Die dabei verarbeiteten Daten sind besonders sensibel. Durch die Aufklärung erhobener Vorwürfe und die anschließend erforderliche Reaktion sind in der Regel mehrere Stellen in die Datenverarbeitung einzubinden.

Die Verarbeitung der dabei verarbeiteten Daten kann sich – je nach Art der Daten und Verarbeitungsvorgang – nach den §§ 32 oder 28 Abs. 1 Nr. 2 BDSG richten.

§ 28 Abs. 1 Nr. 2 BDSG

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

1. …
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder ...

§ 32 BDSG

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Besteht eine Verpflichtung des Unternehmens zur Schaffung eines Hinweisgebersystems, ist die damit zusammenhängende Datenverarbeitung unzweifelhaft zur Wahrung berechtigter Interessen des Unternehmens erforderlich, § 28 Abs. 1 Nr. 2 BDSG. Dennoch sind dabei die berechtigten Interessen der Mitarbeiter zu wahren.

Die datenschutzrechtlichen Aufsichtsbehörden haben sich mit dem Thema Whistleblowing bereits mehrfach befasst und ihre Auffassung auch schriftlich niedergelegt (insbesondere unter https://www.datenschutz-hamburg.de/news/detail/article/whistleblowing-hotlines-firmeninterne-warnsysteme-beschaeftigtendatenschutz.html und http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_de.pdf).

Während in den bisherigen Überlegungen die Daten des Beschuldigten im Vordergrund standen, gab es im vorliegenden Fall vor allem Zweifel an der datenschutzgerechten Verarbeitung der Daten des Mitarbeiters, der einen Vorfall meldet.

So war unklar, an wen genau sich Mitarbeiter wenden können. In dem Bestreben, Meldungen möglichst einfach zu erhalten, waren in der Whistleblowing-Richtlinie zahlreiche Stellen genannt, an die sich ein Mitarbeiter wenden sollte. Darunter waren vor allem auch der direkte Vorgesetzte und die Personalabteilung. Dadurch war nicht sichergestellt, dass sich eine Meldung nicht mit den Personaldaten des betroffenen Mitarbeiters vermischt und keine zweckfremde Nutzung der Daten erfolgt. Auch war unklar, an welchen Stellen im Unternehmen die Daten des meldenden Mitarbeiters letztlich verarbeitet werden, welche Stellen darauf zugreifen können und welche Stelle sicherstellt, dass nur die Mitarbeiter darauf zugreifen können, die mit der Untersuchung des Vorgangs befasst sind.

Bei bisherigen datenschutzrechtlichen Untersuchungen von Hinweisgeber-Systemen wurde deutlich, dass anonyme Mitteilungen im Hinblick auf die beschuldigten Mitarbeiter nicht vollkommen unproblematisch sind. Dies vor allem deshalb, weil sich der Beschuldigte gegen anonyme Vorwürfe schwerer verteidigen kann.

Andererseits ist auch der meldende Mitarbeiter an der vertraulichen Behandlung seiner Daten interessiert. Die Schaffung von Hinweisgebersystemen zielt oft darauf ab, Gesetzesverstöße von Kollegen und Vorgesetzten der meldenden Mitarbeiter zu unterbinden. Meldende Mitarbeiter erfüllen mit der Meldung eine gegenüber ihrem Arbeitgeber bestehende Verpflichtung, wenn sich eine solche aus internen Arbeitsanweisungen wirksam ergibt. Unterlassen sie eine Meldung, obwohl Gesetzesverstöße unübersehbar waren, verstoßen sie gegen den Arbeitsvertrag und müssen mit arbeitsrechtlichen Maßnahmen rechnen. Allerdings müssen Mitarbeiter bei Bekanntwerden der Meldung auch bei berechtigten Meldungen mit Repressalien durch Kollegen und Vorgesetzte rechnen. Daher sind Mitarbeiter, die eine Verpflichtung zur Meldung erfüllen, besonders schutzwürdig. Ihre berechtigten Interessen im Sinne von § 28 Abs. 1 Nr. 2 BDSG sind daher strikt zu wahren.

Das betroffene Kreditinstitut hat nach Gesprächen mit mir die Problematik erkannt und konkrete Änderungen am Verfahrensablauf und deren verbindliche Regelung zugesagt. Dabei soll insbesondere nur noch eine zentrale Stelle mit nur wenigen Personen mit der Entgegennahme von Meldungen betraut werden. Außerdem soll die Behandlung der Daten verbindlich geregelt und die Bearbeitung für meldende Mitarbeiter vor allem durch die Veröffentlichung von schriftlichen Arbeitsanweisungen transparent gemacht werden. Die Bearbeitung dauert noch an.

4.4.7
Telefonaufzeichnung bei einem Zahlungsinstitut

Ausnahmslose Aufzeichnungen erfordern die Einräumung eines Widerspruchsrechts.

Im Berichtszeitraum erreichten mich zwei Beschwerden zur Telefonaufzeichnung bei einem Zahlungsinstitut.

Bei dem Zahlungsinstitut wurden eingehende Telefonate nach einem entsprechenden Hinweis ausnahmslos aufgezeichnet. Die Nachfrage bei dem Zahlungsinstitut ergab, dass die Gesprächsaufzeichnung zur Dokumentation einer Identitätsprüfung bei Erteilung von Auskünften und zur Vermeidung und Vorbeugung von Missbrauch erfolgt. Die aufgezeichneten Gespräche sollten für mindestens acht Monate gespeichert bleiben. Eine Widerspruchsmöglichkeit gegen die Gesprächsaufzeichnung war nicht vorgesehen.

Eine Befugnis zur Aufzeichnung ergibt sich in diesem Fall nur dann aus § 28 Abs. 1 Nr. 2 BDSG, wenn zusätzlich ein Widerspruchsrecht für den Anrufer eingerichtet wird. Durch das Widerspruchsrecht werden die berechtigten Interessen des Kunden gewahrt.

§ 28 Abs. 1 Nr. 2 BDSG

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

1. ...
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder ...

Die Erteilung von Auskünften nur an berechtigte Anrufer dient dem Schutz der Kunden des Zahlungsinstitutes. Die Erteilung von Auskünften an unberechtigte Dritte wäre ein Vertragsverstoß. Die Dokumentation der Identitätsprüfung dient daher auch dem Schutz des Zahlungsinstitutes. Dieses konnte außerdem darlegen, dass es in der Vergangenheit zu diversen Missbrauchsfällen zu Lasten des Zahlungsinstitutes gekommen war. Schutzwürdige Interessen des Zahlungsinstitutes lagen damit vor. Die von dem Zahlungsinstitut angebotene Hotline dient außerdem nur sehr eng begrenzten Zwecken. Der Gesprächsinhalt geht deshalb nie über die Umstände einer konkreten Zahlung und zu deren Status hinaus. Die Aufzeichnung von Gesprächsinhalten mit schutzwürdigen Inhalten ist daher unwahrscheinlich.

Dennoch stehen der Aufzeichnung grundsätzlich die schutzwürdigen Interessen des Anrufers entgegen. Zusätzlich ist zu Lasten des Zahlungsinstitutes zu berücksichtigen, dass gleichwohl eine wenn auch unwahrscheinliche Möglichkeit zur Aufzeichnung von Gesprächsanteilen besteht, die mit der konkreten Zahlung nicht in direktem Zusammenhang stehen. Wird dem Anrufer jedoch die Möglichkeit eingeräumt, der Aufzeichnung zu widersprechen, sind die schutzwürdigen Interessen des Anrufers gewahrt. Diese stehen dann der Aufzeichnung nicht mehr entgegen.

Das Zahlungsinstitut wird das Widerspruchsrecht so kurzfristig technisch umsetzen, wie dies möglich ist. Darüber hinaus wird die Aufzeichnung auf den zulässigen Zeitraum von sechs Monaten begrenzt.

4.4.8
Anforderung von Personalausweisen zur Prüfung von Sanktionslisten

Kreditinstitute dürfen Personalausweiskopien von Zahlungsempfängern, die bei dem Kreditinstitut kein Konto unterhalten, auch zur Prüfung von Sanktionslisten nicht anfordern. Stattdessen können bei dem Kreditinstitut, welches das Konto des Zahlungsempfängers führt, Informationen zum Zahlungsempfänger angefordert werden.

Zur Bekämpfung des Terrorismus bestehen als unmittelbar geltendes Europäisches Recht die sogenannten "Antiterrorismusverordnungen". Dabei handelt es sich um die EU-Verordnungen 881/2002 (ABl. EG Nr. L139, Seite 9), 2580/2001 (ABl. EG Nr. L344, Seite 70) und 753/2011 (ABl. EG Nr. L199, Seite 1). Durch diese drei Verordnungen soll verhindert werden, dass Terroristen oder Terrorverdächtigen Ressourcen zur Unterstützung des Terrorismus zur Verfügung gestellt werden. Aus den EU-Verordnungen gehen wiederum "Sanktionslisten" hervor, die ständig aktualisiert werden. Den auf diesen Listen enthaltenen Personen, Gruppen und Organisationen dürfen weder direkt noch indirekt wirtschaftliche Ressourcen zur Verfügung gestellt werden.

Unter wirtschaftliche Ressourcen im Sinne der EU-Verordnungen fallen unter anderem auch Gehaltszahlungen oder Vergütungen für freie Mitarbeiter. Vor allem Kreditinstitute sind daher verpflichtet, vor der Durchführung von Zahlungen zu prüfen, ob Begünstigte auf einer Sanktionsliste enthalten sind.

Durch die Beschwerde eines Datenschutzbeauftragten wurde ich auf eine daraus resultierende Praxis eines Kreditinstitutes aufmerksam gemacht. In den der Beschwerde zugrunde liegenden Fällen sollten Gehaltszahlungen geleistet werden. Das Kreditinstitut des Arbeitgebers glich dabei die Namen der begünstigten Mitarbeiter mit den Sanktionslisten ab. Bei Namensgleichheiten wurden von den begünstigten Mitarbeitern sodann Kopien der Personalausweise angefordert, um eine Zahlung an auf den Sanktionslisten enthaltene Personen auszuschließen. Dies geschah, obwohl die betroffenen Mitarbeiter bei dem Kreditinstitut des Arbeitgebers keine Konten unterhielten.

Die Anforderung von Kopien von Personalausweisen beurteile ich datenschutzrechtlich generell als kritisch. Für die Anforderung von Personalausweisen muss es hinreichende Gründe und eine Rechtsgrundlage geben. Bei der Eröffnung von Konten stellt nach meiner Auffassung § 8 Abs. 1 Geldwäschegesetz (GwG) eine hinreichende Grundlage für die

Anforderung oder Anfertigung von Personalausweiskopien dar, weil die Erstellung von Kopien zur Dokumentation der obligatorischen Identifizierung bei Kontoeröffnung erforderlich ist. Dies gilt jedoch nur für die Eröffnung von Konten bei der Bank, die zur Identifizierung verpflichtet ist.

§ 8 Abs. 1 GwG

Soweit nach diesem Gesetz Sorgfaltspflichten bestehen, sind die erhobenen Angaben und eingeholten Informationen über Vertragspartner, wirtschaftlich Berechtigte, Geschäftsbeziehungen und Transaktionen aufzuzeichnen. In den Fällen des § 4 Abs. 4 Satz 1 Nr. 1 sind auch die Art, die Nummer und die ausstellende Behörde des zur Überprüfung der Identität vorgelegten Dokuments aufzuzeichnen. Die Anfertigung einer Kopie des zur Überprüfung der Identität vorgelegten Dokuments nach § 4 Abs. 4 Satz 1 Nr. 1 und die Anfertigung einer Kopie der zur Überprüfung der Identität vorgelegten oder herangezogenen Unterlagen nach § 4 Abs. 4 Satz 1 Nr. 2 gelten als Aufzeichnung der darin enthaltenen Angaben; im Falle einer Einsichtnahme auf elektronisch geführte Register- oder Verzeichnisdaten gilt die Anfertigung eines Ausdrucks als Aufzeichnung der darin enthaltenen Angaben.

Für die Anforderung von Personalausweiskopien von Zahlungsempfängern (in diesem Falle der Arbeitnehmer) sehe ich jedoch keine Rechtsgrundlage. Das kontoführende Institut des Zahlungsempfängers ist verpflichtet, einen Abgleich mit den Sanktionslisten vorzunehmen. Hat dieses die geltenden EU-Verordnungen vorschriftsmäßig beachtet, befindet sich der Zahlungsempfänger daher auch bei vorliegenden Namensgleichheiten nicht auf einer Sanktionsliste.

Dies befreit das Kreditinstitut des Zahlungspflichtigen (in diesem Fall der Arbeitgeber) nicht von der eigenen Prüfung. Liegt eine Namensgleichheit vor und bestehen bei dem Kreditinstitut des Zahlungspflichtigen Unsicherheiten über die Person des Zahlungsempfängers, bietet aber § 25h Abs. 3 Kreditwesengesetz (KWG) ausreichende Möglichkeiten, um bei dem kontoführenden Kreditinstitut Angaben über den Zahlungsempfänger anzufordern. Alle benötigten Daten liegen dort bereits vor.

§ 25h Abs. 3 KWG

Jeder Sachverhalt, der nach Absatz 2 Satz 1 als zweifelhaft oder ungewöhnlich anzusehen ist, ist vom Institut zu untersuchen, um das Risiko der jeweiligen Geschäftsbeziehungen oder

Transaktionen überwachen, einschätzen und gegebenenfalls das Vorliegen eines nach § 11 Absatz 1 des Geldwäschegesetzes meldepflichtigen Sachverhalts oder die Erstattung einer Strafanzeige gemäß § 158 der Strafprozessordnung prüfen zu können. Über diese Sachverhalte hat das Institut angemessene Informationen nach Maßgabe des § 8 des Geldwäschegesetzes aufzuzeichnen und aufzubewahren, die für die Darlegung gegenüber der Bundesanstalt erforderlich sind, dass diese Sachverhalte nicht darauf schließen lassen, dass eine Tat nach § 261 des Strafgesetzbuchs oder eine Terrorismusfinanzierung begangen oder versucht wurde oder wird. Absatz 2 Satz 2 gilt entsprechend. Institute dürfen im Einzelfall einander Informationen im Rahmen der Erfüllung ihrer Untersuchungspflicht nach Satz 1 übermitteln, wenn es sich um einen in Bezug auf Geldwäsche, Terrorismusfinanzierung oder einer sonstigen Straftat auffälligen oder ungewöhnlichen Sachverhalt handelt und tatsächliche Anhaltspunkte dafür vorliegen, dass der Empfänger der Informationen diese für die Beurteilung der Frage benötigt, ob der Sachverhalt gemäß § 11 des Geldwäschegesetzes anzuzeigen oder eine Strafanzeige gemäß § 158 der Strafprozessordnung zu erstatten ist. Der Empfänger darf die Informationen ausschließlich zum Zweck der Verhinderung der Geldwäsche, der Terrorismusfinanzierung oder sonstiger strafbarer Handlungen und nur unter den durch das übermittelnde Institut vorgegebenen Bedingungen verwenden.

Ich konnte das Kreditinstitut davon überzeugen, dass die Anforderung von Personalausweiskopien weder erforderlich noch zulässig ist. Das Kreditinstitut hat seine Praxis geändert und mir dies schriftlich bestätigt.

4.4.9
Speicherung von Besucherdaten durch Spielbanken

Spielbanken sind aufgrund verschiedener gesetzlicher Regelungen dazu verpflichtet, die Personalien ihrer Besucher beim Einlass zu kontrollieren und zu speichern. Dabei sind selbstverständlich auch datenschutzrechtliche Grundsätze zu beachten.

Mich erreichte eine Beschwerde über den Umgang einer hessischen Spielbank mit gespeicherten Daten ihrer Besucher. Die Betroffene hatte in den 1990er-Jahren zusammen mit ihrem Ehemann gelegentlich die Spielbank besucht. Damals waren bei der Einlasskontrolle u. a. Namen und Anschrift des Ehepaars erhoben und im System der Spielbank gespeichert worden. Nach dem Jahr 1995 besuchte das Ehepaar die Spielbank nicht mehr, der Ehemann verstarb kurz nach der Jahrtausendwende. Als die Betroffene,

20 Jahre nach ihrem letzten Besuch, im Berichtszeitraum erneut die Spielbank besuchte, wurde ihr am Einlass eine personalisierte Eintrittskarte ausgestellt. Diese enthielt jedoch statt ihres Namens den ihres verstorbenen Ehemanns.

Die Spielbank räumte auf meine Anfrage hin ein, dass das derzeit genutzte Computersystem in den späten 1980er-Jahren eingeführt worden sei und dass alle seitdem erhobenen Besucherdaten noch bei der Spielbank gespeichert seien. Bisher seien Kundendaten lediglich in Einzelfällen gelöscht worden. Zudem wurde erläutert, dass die eingesetzte Software die Möglichkeit vorsieht, die Datensätze von (Ehe-)Partnern, die die Spielbank gemeinsam besucht hatten, miteinander zu verknüpfen. So enthielten die Datensätze vieler Spielbankbesucher Verweise auf den Datensatz ihres als solchen registrierten Partners. Dies sollte bei zukünftigen gemeinsamen Spielbankbesuchen beider Partner eine beschleunigte Einlasskontrolle ermöglichen.

Als die Betroffene im Jahr 2015 die Spielbank besuchte, waren ihre Daten in deren System aufgrund der Besuche in den 90er-Jahren noch vorhanden. Bei der Zutrittskontrolle wurde sie daher als wiederkehrende Spielbankkundin erkannt. Da sich inzwischen jedoch ihre Anschrift geändert hatte, sollten die veralteten Daten von einem Spielbankmitarbeiter aktualisiert werden. Dieser rief aber versehentlich den im Datensatz der Betroffenen vorhandenen Verweis auf den ebenfalls noch gespeicherten Datensatz ihres verstorbenen Ehemanns auf und änderte dessen Adressdaten. Da der Fehler vom Mitarbeiter nicht bemerkt wurde, wurde auch die Eintrittskarte auf den Namen des Ehemannes ausgestellt.

Es gibt verschiedene gesetzliche Regelungen, die Spielbanken aus Gründen der Spielsuchtprävention, des Jugendschutzes und der Geldwäscheprävention dazu zu verpflichten, den Zutritt zu ihren Räumlichkeiten einzuschränken und bei der Zutrittskontrolle Daten ihrer Besucher zu erheben und zu speichern. Dabei dürfen jedoch nur solche Daten erhoben werden, die für eine eindeutige Identifizierung der Besucher erforderlich sind bzw. die in den jeweiligen gesetzlichen Grundlagen ausdrücklich genannt sind.

Die Speicherung des Familienstandes und der Information, wer wessen Partner ist, ist zu diesen Zwecken nicht erforderlich. Daher ist die Verknüpfung der Datensätze von Partnern unzulässig.

Auch dürfen die rechtmäßig erhobenen und gespeicherten Daten nicht ohne jegliche zeitliche Begrenzung gespeichert werden. Wenn Spieler in der sog. Spielersperrdatei eingetragen sind, die dazu dienen soll, spielsüchtige Personen vom Spielen abzuhalten,

gelten für deren Daten spezielle Speicher- bzw. Löschfristen. In allen anderen Fällen sind die Daten gemäß § 35 Abs. 2 S. 2 Nr. 3 BDSG zu löschen, sobald ihre Kenntnis für die Zwecke der Zutrittskontrolle und der Geldwäscheprävention nicht mehr erforderlich ist. Das Geldwäschegesetz sieht in § 8 Abs. 3 S. 1 GwG vor, dass die zur Geldwäscheprävention erhobenen Daten fünf Jahre lang aufzubewahren sind. Eine über diesen Zeitraum hinausgehende Aufbewahrung der Kundendaten ist, auch für die anderen mit der Zutrittskontrolle verfolgten Zwecke, nicht erforderlich. Häufig haben sich nach fünf Jahren bestimmte Daten wie z. B. die Anschrift ohnehin geändert, so dass eine weitere Speicherung solcher alten Daten weder erforderlich noch sinnvoll ist.

In Absprache mit dem für die Spielbankaufsicht zuständigen HMDIS wurde die Spielbank daher aufgefordert, Besucherdaten grundsätzlich fünf Jahre nach Ablauf des Jahres, in dem der letzte Besuch der Spielbank stattgefunden hat, zu löschen. Eine entsprechende Löschroutine wurde daraufhin von der Spielbank eingeführt. Zudem wurden die alten Datensätze aller Kunden gelöscht, die seit über fünf Jahren nicht mehr die Spielbank besucht hatten. Auch schaffte die Spielbank auf meine Aufforderung hin die Verweise auf den Partner des Besuchers ab und löschte die in alten Datensätzen noch bestehenden Verweise.

4.5
Verkehr und Energieversorger

4.5.1
Erteilung der einfachen Registerauskunft durch die Zulassungsstellen

Die Zulassungsstellen sind unter bestimmten, im Straßenverkehrsgesetz geregelten Voraussetzungen zur Auskunftserteilung über die Fahrzeug- und Halterdaten verpflichtet.

Die Zulässigkeit der Auskunftserteilung über die Halterdaten durch die Zulassungsstellen ist immer wieder Gegenstand der Anfragen sowohl seitens der Zulassungsstellen als auch seitens der betroffenen Halter.

Die Fahrzeugregister haben den Zweck, die im öffentlichen Straßenverkehr zugelassenen Fahrzeuge und deren Halter zu registrieren und diese Daten für verkehrsbezogene Belange zur Verfügung zu stellen, § 32 Straßenverkehrsgesetz (StVG). Die einfache Registerauskunft

ist eine der häufigsten Formen der Registerauskunft und ist in § 39 Abs. 1 StVG geregelt. § 39 StVG stellt eine bereichsspezifische, datenschutzrechtliche Regelung dar.

§ 39 Abs. 1 StVG

Von den nach § 33 Abs. 1 gespeicherten Fahrzeugdaten und Halterdaten sind

1. Familienname (bei juristischen Personen, Behörden oder Vereinigungen: Name oder Bezeichnung),
2. Vornamen,
3. Ordens- und Künstlername,
4. Anschrift,
5. Art, Hersteller und Typ des Fahrzeugs,
6. Name und Anschrift des Versicherers,
7. Nummer des Versicherungsscheins oder, falls diese noch nicht gespeichert ist, Nummer der Versicherungsbestätigung,
8. gegebenenfalls Zeitpunkt der Beendigung des Versicherungsverhältnisses,
9. gegebenenfalls Befreiung von der gesetzlichen Versicherungspflicht,
10. Zeitpunkt der Zuteilung oder Ausgabe des Kennzeichens für den Halter sowie
11. Kraftfahrzeugkennzeichen

durch die Zulassungsbehörde oder durch das Kraftfahrt-Bundesamt zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (einfache Registerauskunft).

Auf die Übermittlung von Daten besteht bei Vorliegen der genannten Voraussetzungen ein Rechtsanspruch. Die Halter- und Fahrzeugdaten können von der Zulassungsstelle an private wie öffentliche, inländische wie ausländische Antragsteller übermittelt werden. Die Auskunftserteilung aus dem Fahrzeugregister ist nicht nur in die Mitgliedstaaten der Europäischen Union und in die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zulässig, sondern auch in die Drittstaaten, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist (§ 4c Abs. 1 Nr. 6 BDSG). Adressat der Übermittlung können neben dem Geschädigten eines Verkehrsunfalls und anderen Personen, die Rechtsansprüche aus den verkehrsrechtlichen Verstößen haben könnten, auch Schädiger sein. Dies wird durch die Erwähnung der „Abwehr von Rechtsansprüchen“ im Gesetz deutlich.

Des Weiteren müssen Rechtsansprüche im Zusammenhang mit der Teilnahme am Straßenverkehr vorgetragen werden. Im Zusammenhang mit der Teilnahme am Straßenverkehr stehen auch Parkunfälle im öffentlichen Straßenraum, aber auch auf dem Privatparkplatz. Die Halterauskunft ist auch bei den im Ausland begangenen Verstößen zu erteilen.

Nicht ausreichend ist es dagegen, wenn der Antragsteller lediglich die Eigentümereigenschaft des Halters durch die einfache Registerauskunft bspw. im Rahmen der Zwangsvollstreckungsangelegenheiten feststellen will. Denn der Zweck des Fahrzeugregisters ist es nicht, die Fahrzeuge als Vermögensgegenstände zu erfassen. Der Darlegungspflicht des Antragstellers ist Genüge getan, wenn er plausibel behauptet, dass die Daten mindestens zu einem der in § 39 Abs. 1 StVG genannten Zwecke benötigt werden. Der angegebene Grund wird lediglich auf Plausibilität geprüft und muss nicht glaubhaft gemacht werden, weil das zu einem zu hohen Verwaltungsaufwand bei der Zulassungsbehörde führen würde (Begründung s. BTDrucks. 10/5343, S. 74).

Der landläufig verbreiteten Ansicht, dass die falschen Angaben in diesem Zusammenhang ohne Konsequenz bleiben würden, muss widersprochen werden. Bei falschen Angaben des Antragstellers im Rahmen seiner Darlegungspflicht kann § 43 Abs. 2 Nr. 4 BDSG zum Zuge kommen.

§ 43 Abs. 2 Nr. 4 BDSG

Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
…
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht …

Eine bereichsspezifische Sanktionsregelung existiert im Straßenverkehrsgesetz nicht. In solchen Fällen ist das BDSG subsidiär heranzuziehen. Das bedeutet, dass die nicht abschließende, bereichsspezifische Regelung durch den Rückgriff auf die Sanktionsvorschriften des Bundesdatenschutzgesetzes ergänzt werden darf.

Die zuständige Bußgeldstelle in Hessen ist nach § 24 Abs. 4 HDSG der Hessische Datenschutzbeauftragte.

4.5.2
Führerscheinkontrollen durch den Arbeitgeber

Die vom Arbeitgeber durchzuführenden Führerscheinkontrollen im Falle der Bereitstellung von Dienstfahrzeugen stoßen vielfach auf Unverständnis der Arbeitnehmer. Für die Führerscheinkontrollen existieren gesetzliche Grundlagen.

Das Unterlassen der Fahrerlaubnisprüfung kann strafrechtliche Konsequenzen für den Arbeitgeber gemäß § 21 Abs. 1 Ziff. 2 StVG nach sich ziehen. Dort ist geregelt, dass derjenige mit einer Freiheitsstrafe bis zu einen Jahr oder mit Geldstrafe bestraft werden kann, wer als Halter eines Kraftfahrzeuges anordnet oder zulässt, dass jemand das Fahrzeug führt, der die dazu erforderliche Fahrerlaubnis nicht hat oder dem das Führen eines Fahrzeuges nach § 44 StGB oder nach § 25 StGB verboten ist. Ausreichend für die Erfüllung des Straftatbestands ist bereits die fahrlässige Begehung. Der Arbeitgeber, der einen Dienstwagen – gleichgültig ob personalisiert oder aus einem Fahrzeugpool, dauerhaft oder nur vorübergehend – zur Verfügung stellt, ist Halter des Fahrzeugs. Ihn als Halter trifft demnach die Pflicht, das Dienstfahrzeug nur einer Person zu überlassen, die im Besitz eines gültigen und für die Führung des jeweiligen Dienstfahrzeugs vorgeschriebenen Führerscheins ist.

Das Unterlassen der Überprüfung des Vorhandenseins einer Fahrerlaubnis kann nicht nur strafrechtliche, sondern auch versicherungsrechtliche Konsequenzen nach sich ziehen: Es droht der Verlust des Versicherungsschutzes. Gemäß D 1.1.3 AKB (Allgemeine Bedingungen für die Kraftfahrzeugversicherung) wird der Versicherer von der Leistung frei, wenn der Halter oder der Eigentümer das Fahrzeug von einem Fahrer benutzen lässt, der nicht die erforderliche Fahrerlaubnis hat. Verstöße gegen die Kontrollpflicht führen also dazu, dass die Kfz-Haftpflichtverletzung im Falle eines Unfalles zwar den Schaden dem Geschädigten ersetzen muss, aber anschließend beim Versicherungsnehmer für die Obliegenheitsverletzung Regress nehmen kann.

Grundsätzlich ist es nicht ausreichend, bei erstmaliger Überlassung eines Kraftfahrzeuges an eine andere Person sich den Führerschein zur Einsicht vorlegen zu lassen. Auch eine Regelung im Fahrzeug-Überlassungsvertrag oder im Arbeitsvertrag, wonach der Verlust des Führerscheins dem Arbeitgeber unverzüglich mitzuteilen ist, ist zwar zu empfehlen, entbindet aber den Arbeitgeber nicht von seiner Halterverantwortung nach § 21 StVG. Hier muss der Arbeitgeber berücksichtigen, dass Mitarbeiter aus Angst vor einem Jobverlust den Entzug

der Fahrerlaubnis verschweigen könnten. Vielmehr muss sich der Arbeitgeber durch die regelmäßige, schriftlich dokumentierte Einsichtnahme in den Führerschein im Original davon überzeugen, dass der Fahrzeugführer die zutreffende Fahrerlaubnis (noch) hat. Der Arbeitgeber muss ein schlüssiges Konzept vorlegen können, mit dem ihm der Nachweis der Erfüllung seiner Sorgfaltspflichten aus dem Straßenverkehrsgesetz gelingt.

Das Verfahren der Führerscheinprüfungen ist abhängig von der Anzahl der Fahrzeuge, Anzahl der Fahrer, Art der Fahrzeugnutzung und vielfältigen anderen Faktoren. Ein Musterprüfungsverfahren kann hier daher nicht vorgeschlagen werden. Grundsätzlich halte ich die halbjährliche Kontrolle der Originaldokumente datenschutzrechtlich für angemessen. Die Erstellung der Führerscheinkopien und ihre Ablage in den Personalakten können unter besonderen Umständen auch erforderlich sein.

Die tatsächliche Kontrolle kann entweder durch den Arbeitgeber selbst oder durch entsprechende Dienstleister durchgeführt werden. Sollten Letztere eingesetzt werden, ist zu beachten, dass ein Vertrag zur Auftragsdatenverarbeitung nach § 11 BDSG notwendig sein kann.

4.5.3
Datenverarbeitung im Rahmen der Stromgrundversorgung

Die Stromgrundversorger sind aufgrund der Möglichkeit des konkludenten Abschlusses des Grundversorgungsvertrages und der damit einhergehenden Unkenntnis über die Identität des Vertragspartners/Verbrauchers mit datenschutzrechtlichen Herausforderungen konfrontiert.

Energieunternehmen in ihrer Funktion als Stromgrundversorger fragten Namen und Adressen der Nachmieter und der Vermieter der Wohnung bei ausziehenden Vormietern in der Kündigungsbestätigung pauschal ab. Dagegen sind bei mir mehrere Beschwerden von betroffenen Bürgern eingegangen.

Im Rahmen der gesetzlich vorgeschriebenen Stromgrundversorgung sieht der Gesetzgeber vor, dass Personen, die sich um keinen Stromanbieter kümmern, dem Grundversorger als Kunden zugewiesen werden und mit Strom versorgt werden [§ 1 Abs. 3 Verordnung über Allgemeine Bedingungen für die Grundversorgung von Haushaltskunden und die Ersatzversorgung mit Elektrizität aus dem Niederspannungsnetz

(Stromgrundversorgungsverordnung/StromGVV) in Verbindung mit § 36 Abs. 1 des Gesetzes über die Elektrizität- und Gasversorgung (Energiewirtschaftsgesetz/EnWG)].

Grundversorger ist jeweils das Energieunternehmen, das die meisten Haushaltskunden in einem Netzgebiet der allgemeinen Versorgung beliefert (§ 36 Abs. 2 EnWG). Dabei kommt es im Falle der netzgebundenen Versorgung zu einem konkludent geschlossenen Vertragsverhältnis (Grundversorgungsvertrag) zwischen Grundversorger und Haushaltskunde, wenn der Kunde die Energie aus dem Elektrizitätsversorgungsnetz entnimmt (§ 2 Abs. 2 StromGVV). Im Rahmen der Grundversorgung stellt die Energieentnahme den Regelfall der Vertragsbegründung.

Beim Auszug des Kunden aus einer Wohnung wird ein neuer Grundversorgungsvertrag durch Entnahme von Strom entweder mit dem Nachmieter oder bei Leerstand zunächst mit dem Vermieter der betreffenden Wohnung begründet. In einer derartigen Konstellation ist der Kunde verpflichtet, dem Grundversorger die Entnahme der Elektrizität unverzüglich in Textform mitzuteilen (§ 2 Abs. 2 StromGVV). Der Grundversorger ist seinerseits dazu verpflichtet, dem Vertragspartner den Abschluss eines Grundversorgungsvertrages schriftlich zu bestätigen. Die Mitteilungen der Kunden bleiben bedauerlicherweise in den meisten Fällen aus, so dass der Grundversorger vor der Herausforderung steht, einen konkludent geschlossenen Grundversorgungsvertrag bestätigen zu müssen, ohne dass ihm der Vertragspartner bekannt ist. In Anbetracht der großen Anzahl von Kundenwechseln ist der Grundversorger darauf angewiesen, ohne großen Aufwand, insbesondere ohne Sachverhaltsaufklärung vor Ort, Kenntnis von dem neuen Vertragspartner und seinen Adressdaten (des Vermieters) zu erlangen.

Die Schreiben an die jeweiligen Versorgungsadressen sind ohne Kenntnis der Namen der Strombezieher bei Mehrfamilienhäusern unzustellbar. Die Auskünfte aus den Liegenschaftskatastern und Grundbüchern enthalten oft veraltete Adressen der Eigentümer. Denn die Immobilieneigentümer sind nicht verpflichtet, beim Umzug ihre neue Adresse beim Grundbuchamt oder beim Amt für Bodenmanagement zu melden. Auch die Auskünfte aus dem Einwohnermelderegister bringen nicht das erwünschte Ergebnis. Die Meldungen des Wohnungswechsels werden gerade von den Personen, die auch die Mitteilung der Stromentnahme unterlassen, nicht oder nicht in der vorgesehenen Frist nach dem Umzug getätigt. Aus diesen Gründen sind manche Stromgrundversorger dazu übergegangen, den ausziehenden Vormieter nach den für den Grundversorgungsvertrag relevanten Daten pauschal in der Kündigungsbestätigung zu fragen.

§ 28 Abs. 1 Nr. 1 BDSG kommt als datenschutzrechtliche Grundlage für eine derartige Datenerhebung nicht infrage, da zum Zeitpunkt der Abfrage meist noch kein Grundversorgungsvertrag mit einem Nachmieter/Eigentümer existiert. Als datenschutzrechtliche Rechtsgrundlage für die Erhebung der Namen und Adressen der Nachmieter und der Wohnungseigentümer kommt aber § 28 Abs. 1 Nr. 2 BDSG in Betracht. Angesichts des niedrigen Sensibilitätsgrades der abgefragten Daten, der Erfahrung der fehlenden Mitteilungen der Stromentnahmen, des vom Grundversorger betriebenen Massengeschäfts und seiner überschaubaren Möglichkeiten, an die vertragsrelevanten Daten des Nachmieters oder des Eigentümers zu kommen, fällt die Interessenabwägung zugunsten der erhebenden Stelle aus.

Der Grundsatz der Direkterhebung beim Betroffenen (§ 4 Abs. 2 BDSG) wird durch den Ausnahmetatbestand des „unverhältnismäßigen Aufwandes“ eingeschränkt (§ 4 Abs. 2 Satz 2 Nr. 2b BDSG), weil die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand in Form der Vorort-Recherchen bedeuten würde und bei einer Vielzahl von mehreren Zehntausend Kundenwechseln die Notwendigkeit einfacherer und schnellerer Verfahrensweisen besteht.

Die Abfrage von Daten in der Kündigungsbestätigung ist unter folgenden Voraussetzungen zulässig:

– Die Daten dürfen nur abgefragt werden, wenn sie – auch im Massengeschäft – in dem jeweiligen Einzelfall für die Vertragsbearbeitung benötigt werden. Versenden von pauschalen Abfragen an alle ausziehenden Vormieter mit der Aufforderung der Datenübermittlung ist datenschutzrechtlich nicht zulässig.

– Der ausziehende Vormieter muss auf die Freiwilligkeit der Bekanntgabe der abgefragten Angaben im Kündigungsschreiben hingewiesen werden.

Von den Grundversorgern wurden die Musterschreiben meinen Anforderungen angepasst.

4.6
Versicherungswirtschaft

4.6.1
Juristische Personen und Datenschutz

Das Recht auf informationelle Selbstbestimmung steht nur natürlichen Personen zu. Juristische Personen (Unternehmen) können sich demzufolge nicht darauf berufen, in diesem Grundrecht verletzt zu sein. Auch das BDSG verleiht Unternehmen grundsätzlich keine eigene Rechtsposition. Ein Versicherer kann sich daher zulässigerweise nicht darauf berufen, in seinen Rechten nach dem BDSG verletzt zu sein.

4.6.1.1
Beschwerdegegenstand

Ein Unternehmen, das sich an mich wandte, hatte bei einem Versicherer einen Kreditversicherungsvertrag abgeschlossen. Ein anderes Unternehmen stellte an dieses finanzielle Forderungen. Der Versicherer nahm vor diesem Hintergrund mit dem Beschwerde führenden Unternehmen Kontakt auf, um die finanziellen Fragen zu klären.

Daraufhin untersagte das Beschwerde führende Unternehmen dem Versicherer, mit dieser Thematik zu anderen Unternehmen in Kontakt zu treten, weil es eine Rufschädigung (insbesondere betr. seine Kreditwürdigkeit) befürchtete. Der Versicherer nahm zwecks Abwicklung der Angelegenheit gleichwohl Kontakt mit anderen Stellen auf. Daraufhin verständigte das Beschwerde führende Unternehmen wegen der befürchteten Rufschädigung die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), damit diese gegen den Versicherer einschreite. Die BaFin lehnte dies ab und verwies zu dem Thema Rufschädigung (Kreditwürdigkeit) an meine Behörde.

4.6.1.2
Rechtliche Bewertung

Einem Unternehmen, das um Kreditwürdigkeit fürchtet und sich gegen Rufschädigung zur Wehr setzt, kann mit Mitteln des Datenschutzrechts nicht geholfen werden.

Zweck des Bundesdatenschutzgesetzes ist es nämlich, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG).

Um diese Thematik ging es bei der Eingabe aber nicht: Der Ruf eines Unternehmens (z. B. die Kreditwürdigkeit) ist keine Datenschutzfrage im Sinne des Bundesdatenschutzgesetzes (vgl. etwa Gusy in Wolff/Brink, Datenschutzrecht in Bund und Ländern, § 1 BDSG, Rdnr. 44).

Betriebs- und Geschäftsgeheimnisse von Unternehmen sind grundsätzlich nicht nach Datenschutzrecht zu beurteilen.

Datenschutzrechtlich sind ausnahmsweise im Sozialrecht Betriebs- und Geschäftsgeheimnisse personenbezogenen Daten gleichgestellt, §§ 35 Abs. 4 SGB I, 67 Abs. 1 S. 2 SGB X (näher hierzu etwa Steinbach in Hauck/Noftz, SGB I, Rdnr. 57 ff.).

§ 35 SGB Abs. 4 SGB I

Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.

§ 67 Abs. 1 Satz 2 SGB X

Betriebs- und Geschäftsgeheimnisse sind alle betriebs- und geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.

Bei der vorliegenden Eingabe ging es allerdings nicht um das Sozialrecht.

Ich habe das Unternehmen über die Rechtslage informiert. Der Petent ist gehalten, sich erneut an die BaFin zu wenden.

4.6.2
Versicherungswirtschaft – Funktionsübertragung auf Dienstleister

Soweit Versicherungen Aufgaben auf andere Unternehmen übertragen und damit verbunden personenbezogene Daten der Versicherungsnehmer übermitteln, ist diese Datenübermittlung nur ausnahmsweise unzulässig.

4.6.2.1
Beschwerdegegenstand

Eine Bürgerin beschwerte sich mit ihrer Eingabe darüber, dass ihr Versicherer die Wahrnehmung der Sparte Rechtsschutzversicherung auf ein anderes Versicherungsunternehmen übertragen und damit verbunden gegen ihren Willen und trotz ihres pauschalen Widerspruchs personenbezogene Daten an dieses Unternehmen übermittelt hatte.

4.6.2.2
Rechtliche Bewertung

Die Übermittlung personenbezogener Daten ist in § 28 BDSG geregelt.

§ 28 Abs. 1 und 2 BDSG

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

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,
2. soweit es erforderlich ist,
   a) zur Wahrung berechtigter Interessen eines Dritten oder

b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Für die Versicherungswirtschaft wird diese Vorschrift durch sogenannte Verhaltensregeln (Code of Conduct; CoC) u. a. hinsichtlich der Ausgliederung von Versicherungsleistungen näher konkretisiert. Rechtsgrundlage für solche branchenspezifischen, datenschutzrechtlichen Verhaltensregeln ist § 38a BDSG.

§ 38a BDSG

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Art. 22 dieser Verhaltensregeln (CoC) befasst sich mit der Funktionsübertragung auf Dienstleister näher:

Art. 22 Abs. 2 und 3 CoC

(2) Die Übermittlung von personenbezogenen Daten an Dienstleister zur eigenverantwortlichen Erfüllung von Datenverarbeitungs- oder sonstigen Aufgaben kann auch dann erfolgen, wenn dies zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse des Betroffenen dem entgegensteht. Das kann zum Beispiel der Fall sein, wenn Dienstleister Aufgaben übernehmen, die der Geschäftsabwicklung des Unternehmens dienen, wie beispielsweise die Risikoprüfung, Schaden- und

Leistungsbearbeitung, Inkasso mit selbständigem Forderungseinzug oder die Bearbeitung von Rechtsfällen und die Voraussetzungen der Absätze 4 bis 7 erfüllt sind.

(3) Die Übermittlung von personenbezogenen Daten an Dienstleister nach Absatz 1 und 2 unterbleibt, soweit der Betroffene dieser widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse des übermittelnden Unternehmens überwiegt. Die Betroffenen werden in geeigneter Weise darauf hingewiesen.

Vorliegend dient die Auslagerung der Geschäftssparte „Rechtsschutzversicherung“ der Geschäftsabwicklung der Versicherung.

Die Eingeberin hatte der Datenübermittlung nur pauschal widersprochen, ohne eine besondere persönliche Situation darlegen zu können. Schutzwürdige Interessen waren daher nicht zu erkennen. Demzufolge war die Datenübermittlung auch nicht wegen des Widerspruchs unzulässig. Zudem wird im Versicherungsaufsichtsgesetz die Auslagerung der Sparte Rechtsschutzversicherung speziell geregelt.

§ 8a Abs. 1 VAG

Ein Versicherungsunternehmen, das die Rechtsschutzversicherung zusammen mit anderen Versicherungssparten betreibt, hat die Leistungsbearbeitung in der Rechtsschutzversicherung einem anderen Unternehmen (Schadenabwicklungsunternehmen) zu übertragen. Die Übertragung gilt als Funktionsausgliederung.

Diese Regelung soll möglichen Interessenkollisionen beim Versicherer vorbeugen. Wenn beispielsweise nach einem Verkehrsunfall gegen den Versicherer Haftpflichtansprüche vom Unfallgeschädigten geltend gemacht werden und der Unfallgeschädigte dafür zugleich seine Rechtsschutzversicherung beansprucht: Darüber soll dann nicht „im gleichen Hause“ entschieden werden (näher hierzu Kaulbach in Fahr/Kaulbach/Bähr/Pohlmann, VAG, § 8a VAG, Rdnr. 1 ff.).

Die anfragende Bürgerin habe ich über diese Sach- und Rechtslage informiert.

4.7
Wohnungswirtschaft

4.7.1
Sperrung von Daten bei Kündigung eines Immobilienmaklervertrages

Kündigt der Kunde eines Immobilienmaklers die vertragliche Beziehung, dürfen die Daten des Kunden grundsätzlich nicht gelöscht, sondern müssen gesperrt werden.

4.7.1.1
Beschwerdegegenstand

Ein Bürger fragte an, ob er von seinem bisherigen Immobilienmakler fordern könne, dass die den Bürger betreffenden Daten gelöscht werden. Der Kunde habe den Maklervertrag gekündigt und er wolle in Zukunft keine geschäftliche Beziehung mehr mit diesem Makler eingehen.

4.7.1.2
Rechtliche Bewertung

Unbefristete Immobilienmaklerverträge können vom Kunden des Maklers jederzeit gekündigt werden, während der Makler engeren rechtlichen Bindungen unterliegt (hierzu näher bspw. Fehrenbacher in Harz/Riecke/Schmid, Miet- und Wohnungseigentumsrecht, S. 1564 Rdnr. 24).

Die Frage, ob eine solche Kündigung die Löschung der Kundendaten als datenschutzrechtliche Folge auslöst, ist in § 35 BDSG beantwortet.

Danach müssen personenbezogene Daten, die für eigene Zwecke verarbeitet werden, gelöscht werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 S. 2 Nr. 3 BDSG).

§ 35 Abs. 2 Nr. 3 BDSG

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,

...

Mit Blick auf die Kundendaten tritt diese Situation für den Makler ein, wenn ein Vertrag seitens des Kunden gekündigt und die Rechtsbeziehung vom Kunden nachhaltig beendet worden ist.
Eine Löschung scheidet dann aber dennoch aus, soweit Aufbewahrungsfristen bezüglich der angefallenen Vertragsdaten rechtlich angeordnet sind (§ 35 Abs. 3 Nr. 1 BDSG). In diesem Fall wird das Löschungsgebot durch ein Sperrungsgebot ersetzt.

§ 35 Abs. 3 Nr. 1 BDSG

1. An die Stelle einer Löschung tritt eine Sperrung, soweit
   einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

...

Gesetzliche Vorschriften in diesem Sinne sind insbesondere die handelsrechtliche Vorschrift § 257 HGB und die abgabenrechtliche Regelung in § 147 AO. In diesen Normen ist festgelegt, dass Handels- und Geschäftsbriefe sechs Jahre aufzubewahren sind (§ 257 Abs. 4 HGB, § 147 Abs. 3 AO).

§ 257 Abs. 1 und 4 HGB

(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

...

2. die empfangenen Handelsbriefe

Wiedergaben der abgesandten Handelsbriefe

(4) Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren.

§ 147 Abs. 1 und 3 AO

(1) Die folgenden Unterlagen sind geordnet aufzubewahren:
...
2. die empfangenen Handels- und Geschäftsbriefe
3. Wiedergaben der abgesandten Handels- und Geschäftsbriefe,
...

(3) Die in Abs. 1 Nr. 1, 4 und 4a aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren, ...

Die als Folge der Aufbewahrungspflicht verbotene Löschung von personenbezogenen Daten und die stattdessen angeordnete Sperrung bedeuten eine Einschränkung der zulässigen Verwendbarkeit dieser personenbezogenen Daten (§ 35 Abs. 8 BDSG).

§ 35 Abs. 8 BDSG

Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt und genutzt werden dürften, wenn sie nicht gesperrt wären.

Ich habe den Bürger über die Rechtslage informiert.

4.7.2
Wohnungseigentümer und Datenübermittlung durch Verwalter an einen Dritten

Der Verwalter ist gegenüber den Wohnungseigentümern und gegenüber der Gemeinschaft der Wohnungseigentümer nicht ermächtigt, ohne deren Auftrag ihre personenbezogenen Daten an einen Finanzmakler zu übermitteln.

4.7.2.1
Beschwerdegegenstand

Ein Wohnungseigentümer beschwerte sich bei mir darüber, dass der Verwalter der Eigentumswohnanlage personenbezogene Daten aller Wohnungseigentümer an einen Finanzmakler weitergegeben hatte, um ohne Auftrag der Wohnungseigentümer ein Finanzierungsprojekt einzuleiten. Hintergrund waren geplante Sanierungs-/Renovierungsmaßnahmen an der Wohnanlage.

4.7.2.2
Rechtliche Bewertung

Der Verwalter ist gegenüber den Wohnungseigentümern und gegenüber der Gemeinschaft der Wohnungseigentümer u. a. berechtigt und verpflichtet, die für die ordnungsmäßige Instandhaltung und Instandsetzung des gemeinschaftlichen Eigentums erforderlichen Maßnahmen zu treffen (§ 27 Abs. 1 Nr. 2 WEG) und vor allem Beschlüsse der Wohnungseigentümer durchzuführen (§ 27 Abs. 1 Nr. 1 WEG).

§ 27 Abs. 1 WEG

Der Verwalter ist gegenüber den Wohnungseigentümern und gegenüber der Gemeinschaft der Wohnungseigentümer berechtigt und verpflichtet,

1. Beschlüsse der Wohnungseigentümer durchzuführen und für die Durchführung der Hausordnung zu sorgen;
2. die für die ordnungsmäßige Instandhaltung und Instandsetzung des gemeinschaftlichen Eigentums erforderlichen Maßnahmen zu treffen;

...

Die Berechtigung und Verpflichtung zur Instandhaltung und Instandsetzung enthält aber nicht die Befugnis, ohne Mitwirkung der Wohnungseigentümer deren personenbezogene Daten an Dritte weiterzugeben.

Vielmehr hat der Verwalter die Wohnungseigentümer bei seinen Maßnahmen prinzipiell mit einzubinden. Eine Ausnahme bestünde lediglich im Fall der „Notgeschäftsführung“ (näher hierzu etwa Abramenko in Harz/Riecke/Schmid, Miet- und Wohnungseigentumsrecht, Kapitel 19, Rdnr. 64f.; Bärmann/Pick, WEG, § 27 Rdnr. 9).

Im vorliegenden Fall war es so, dass weder ein Beschluss der Wohnungseigentümer noch ein „Notfall“ vorlag, der die Weitergabe personenbezogener Daten der Wohnungseigentümer an den Finanzmakler gerechtfertigt hätte.

Über diese Rechtslage habe ich den Eingeber und den Verwalter informiert.

4.8
Gesundheitswesen

4.8.1
Datenverarbeitung durch eine Blutspendeeinrichtung

Beim Informationsbesuch in einem Blutspendezentrum in Hessen wurde festgestellt, dass Unklarheiten hinsichtlich der Frage bestehen, wer die verantwortliche Stelle für die Datenverarbeitung ist. Zugleich war auch für die Blutspender nicht hinreichend transparent genug, bei welcher Stelle die erhobenen Daten abgelegt werden.

4.8.1.1
Ausgangslage

Anlass für meinen Besuch war die Eingabe eines Ehepaares. Wie mir dieses berichtete, fand es sich zwecks einer Blutspende in dem Blutspendezentrum ein. Nachdem das Ehepaar vor Ort den Anamnesebogen ausgefüllt hatte, wurde es zunächst gebeten, Platz zu nehmen. Da den beiden die Wartezeit zu lange war, und man ihnen andere Personen am Empfang vorzog, entschlossen sie sich kurzerhand dazu, die Blutspende abzubrechen. Beide baten daher darum, dass die im Anamnesebogen bereits erhobenen Daten vernichtet werden und keine Speicherung vorgenommen wird. Daraufhin teilten ihnen Mitarbeiter des Blutspendezentrums mit, dass dies nicht möglich sei, da das Transfusionsgesetz auch eine Speicherung der Daten vorsieht, wenn es tatsächlich nicht zu einer Spende gekommen ist. Hiermit wolle man insbesondere erreichen, dass auf diesem Weg mögliche Risikospender erfasst und bei einem erneuten Besuch nicht zugelassen werden.

Zunächst habe ich mir schriftlich die Vorgänge im Blutspendezentrum darlegen lassen, um mir sodann auch vor Ort ein Bild von den Abläufen zu machen. Hierbei wurde festgestellt,

dass das Blut eigentlich im Auftrag und im Namen einer Einrichtung aus einem anderen Bundesland gewonnen wird. Die tatsächlich die Daten erhebende und speichernde Stelle tauchte jedoch nur auf dem Anamnesebogen erkennbar für den Spender auf.

Darüber hinaus habe ich festgestellt, dass die Blutspendeeinrichtung bislang keinen Datenschutzbeauftragten bestellt hatte, obwohl sie etwa 100 Mitarbeiter beschäftigt und seit ca. zehn Jahren besteht. Die Funktion des Datenschutzbeauftragten übte bislang der Geschäftsführer aus.

4.8.1.2
Rechtliche Bewertung und getroffene Maßnahmen

4.8.1.2.1
Verantwortliche Stelle für die Datenverarbeitung

Um die Verantwortlichkeiten genauer abklären zu können, habe ich mir zunächst den Kooperationsvertrag zwischen der Blutspendeeinrichtung und der Einrichtung aus NRW vorlegen lassen. Die in dem Vertrag festgehaltenen Vereinbarungen enthielten keine klare Antwort auf die Frage, wer die verantwortliche Stelle ist. Insbesondere war in dem Vertrag nicht geregelt, welcher Stelle die Daten gehören, wer für die inhaltliche Richtigkeit der Daten verantwortlich ist, wer für welche Maßnahmen zur Gewährleistung der Datensicherheit verantwortlich ist und welche Stelle auf welche Art und Weise Zugriff auf die Daten hat. In § 4 des Kooperationsvertrages war beispielsweise nicht genau ausgeführt, wie der Zugriff auf das EDV-Spendenmodul der Einrichtung in NRW ausgestaltet ist. Dort hieß es lediglich: *„Die Aufnahme der Spender einschließlich aller relevanten persönlichen und medizinischen Daten erfolgt in das EDV-Spendenmodul der Einrichtung in NRW. “*

Auch der § 2 des Kooperationsvertrages stellte nur fest, dass die Blutspendeeinrichtung in Hessen die Standardarbeitsanweisungen der Einrichtung in NRW zu beachten hat. Darüber hinaus war jedoch nicht genauer geregelt, welche Einflussmöglichkeiten außerhalb dieser Anweisungen bestehen.

Ich habe daher zunächst darum gebeten, dass der Vertrag im Rahmen einer vertraglichen Erweiterung ergänzt wird.

Auch für den Spender selbst ist es entsprechend transparent zu machen, wo seine erhobenen Daten abgelegt werden und welche Einrichtung einen Zugriff darauf hat. Hierüber war aus meiner Sicht gesondert in einem Informationsblatt für den Patienten aufzuklären.

Eine entsprechende Umsetzung beider Punkte wurde mir von dem Unternehmen zugesagt.

4.8.1.2.2
Aufklärung der Spender über die Speicherung der Daten im Falle des Spendenabbruchs

Schließlich habe ich auch darauf Wert gelegt, dass der Patient zumindest vor der Spende darüber informiert wird, dass seine Daten auch im Falle des vorzeitigen Spendenabbruchs gespeichert werden können.

Dem Transfusionsgesetz lässt sich letztlich nicht entnehmen, dass Daten von Patienten, die sich dazu entschließen, nicht zu spenden und die keine Risikopatienten sind, dauerhaft gespeichert werden müssen. Ich habe deshalb gefordert, dass man in solchen Fällen noch einmal eine Einzelfallprüfung vornimmt. Sofern es sich den Angaben nach nicht um Risikopatienten handelt, sind die bereits erhobenen Daten auch zu löschen. Eine weitere Speicherung ist in diesen Konstellationen nicht erforderlich.

Die Blutspendeeinrichtung hat sich dazu bereit erklärt, dies an die verantwortliche Stelle in NRW heranzutragen und eine entsprechende Änderung anzuregen.

4.8.1.2.3
Bestellung eines Datenschutzbeauftragten

Besonders schwer wiegt aus meiner Sicht der Umstand, dass die Blutspendeeinrichtung seit über zehn Jahren keinen eigenen Datenschutzbeauftragten bestellt hat. Dies ist insbesondere deshalb so beachtlich, da im gegebenen Fall die Verarbeitung einer Vielzahl von besonders sensiblen Daten betroffen ist. Wer bereits eine Blutspende vorgenommen hat, weiß, wie detailliert die Anamnesebogen den Spender zu seiner Gesundheit und zu seinem Sexualleben befragen.

Da das Haus auch über 100 Mitarbeiter beschäftigt, die ständig mit der automatisierten Verarbeitung von personenbezogenen Daten befasst sind, finden die §§ 4f, 4g BDSG auch eine entsprechende Anwendung.

Ich habe die Blutspendeeinrichtung in Hessen schließlich darauf hingewiesen, dass der Geschäftsführer eines Unternehmens den Posten des Datenschutzbeauftragten nicht selber ausfüllen kann. Auf meiner Homepage findet sich ein Merkblatt, dem die Mindestanforderungen zu entnehmen sind, die an betriebliche Datenschutzbeauftragte zu stellen sind. Danach sind insbesondere Interessenkonflikte zu vermeiden, die sich aus entsprechenden Doppelfunktionen ergeben können.

Soweit dieser Punkt betroffen ist, werde ich den Vorgang zur weiteren Prüfung und gegebenenfalls Ahndung an die Bußgeldstelle in meinem Haus weiterleiten.

4.8.2
Datenschutzrechtliche Mängel beim Einsatz von Evaluationsbogen bei psychiatrischen Behandlungen

In einer hessischen Klinik erhielt jede Patientin und jeder Patient zu Beginn der Behandlung einen umfangreichen Fragebogen. Der Zweck der Befragung und die weitere Verarbeitung der Daten waren unklar und nicht korrekt dargestellt. Aufgrund meiner Forderungen wurde das Verfahren neu gestaltet und die erforderliche Transparenz hergestellt.

4.8.2.1
Ausgangslage

Der Eingebende berichtete mir, dass er in einer Klinik in Hessen als Patient in der Abteilung Psychosomatik aufgenommen wurde. Gleich zu Beginn seiner Behandlung erhielt er dort von der behandelnden Chefärztin einen Fragebogen mit der Überschrift „Befragung von Patientinnen und Patienten zu Beginn einer stationären psychosomatischen Behandlung“. Auf dem Fragebogen waren Felder für die Patientennummer und das Aufnahmedatum vorgesehen. Auf dem Kopfbogen war zudem ein Universitätsklinikum aus einem anderen Bundesland angegeben.

Wie mir der Eingebende mitteilte, erfolgte nur eine mündliche Information zu der psychologischen Testung. So sei ihm von den Mitarbeitern des Hauses versichert worden, dass die Erhebung und Auswertung in anonymisierter Form erfolgte. Der Eingebende hat jedoch darauf hingewiesen, dass auf dem jeweiligen Fragebogen auch die Patientennummer und das Datum der Aufnahme vermerkt waren. Obwohl er seine Patientennummer hat streichen lassen, wurde diese nach seinen Angaben nachträglich wieder vom Personal der Klinik hinzugefügt. Auf seine hier wiedergegebene Kritik hin habe ihm eine Angestellte der Klinik nahegelegt, seine Behandlung zu beenden und abzureisen.

Unklar war zunächst, wer im gegebenen Fall die verantwortliche Stelle hinsichtlich des Fragebogens ist, welchen Zweck der Fragebogen hat, wie die Daten weiterverarbeitet werden und was passiert, wenn der Fragebogen nicht ausgefüllt wird. Klärungsbedürftig war auch, ob tatsächlich von „anonymisierten“ Daten gesprochen werden konnte. Vor diesem Hintergrund habe ich den Datenschutzbeauftragten der Klinik um Stellungnahme gebeten.

Dieser teilte mir schließlich mit, dass der thematisierte Fragebogen Bestandteil der Behandlung in der Klinik ist. Es handele sich um eine freiwillige standardisierte psychologische Testbefragung, die das Universitätsklinikum entwickelt hat und die regelmäßig entsprechend den neuesten wissenschaftlichen Standards überarbeitet und ausgewertet wird. Die Auswertung erfolge im Universitätsklinikum, mit dem diesbezüglich ein Kooperationsvertrag besteht.

Nach Durchsicht der ergänzend hierzu übersandten Unterlagen habe ich festgestellt, dass die Informationen für den Patienten teilweise nicht korrekt und insgesamt nicht ausreichend waren. Der bestehende Kooperationsvertrag räumte dem Universitätsklinikum darüber hinaus zu weitreichende Rechte ein.

4.8.2.2
Unsere Forderungen/Getroffene Maßnahmen

4.8.2.2.1
Transparenz für die Teilnehmer

Rechtlich war es zunächst unabdingbar, dass die Teilnehmer über den Zweck der Befragung informiert werden sowie darüber, dass die Daten die Klinik verlassen.

Aufgrund der Verbindung des Fragebogens mit der Patientennummer als auch dem Datum der Aufnahme konnte die Befragung auch nicht mehr als anonym bezeichnet werden. Es war daher klarzustellen, dass der Fragebogen zwar durchaus innerhalb der Klinik einer Person zugeordnet werden kann, die Antworten jedoch getrennt von den personenbezogenen Daten ausgewertet und bearbeitet werden.

Damit auch tatsächlich davon ausgegangen werden kann, dass der Patient eine informierte Einwilligung abgegeben hat, habe ich gefordert, dass der Patient über die genaueren Umstände der Befragung in einem gesonderten Papier informiert wird, welches dem Fragebogen beigefügt wird. Darin war auch anzusprechen, ob, in welcher Form und ggf. zu welchem Zweck die Fragebogen im Hause des Universitätsklinikums verbleiben.

In dem mir schließlich übersandten Informationsblatt wurde oftmals von einer Verwendung von „pseudonymisierten Daten“ gesprochen. In Anbetracht des Umfangs des Fragebogens und des damit entstehenden Datensatzes war es aus meiner Sicht jedoch äußerst fraglich, ob eine hinreichende Pseudonymisierung vorliegt. Ich habe daher darum gebeten, dass dieser Begriff vermieden wird. Vielmehr ist dem Patienten mitzuteilen, dass sein Name und seine Adresse nicht weitergegeben werden und in der Klinik verbleiben.

Aufgefallen ist mir in diesem Kontext auch, dass dem Patienten im Informationsblatt zugesichert wird, dass von den Daten, die außerhalb der Klinik ausgewertet werden, keine Rückschlüsse auf die Person möglich sind. In Anbetracht des Umfangs der erhobenen Daten hatte ich Zweifel, dass eine solche Zusicherung tatsächlich für jeden Fall getroffen werden kann. Daher war es hier rechtlich nur möglich, dem Patienten eine strikt zweckgebundene Verwendung der Daten zuzusichern.

4.8.2.2.2
Überarbeitung des Fragebogens

Sowohl das Datum der Aufnahme als auch die Patientennummer befanden sich auf dem Fragebogen. Das Datum der Aufnahme sollte jedoch auf keinen Fall weitergegeben werden, weil damit zusätzliche Reidentifikationsrisiken verbunden sind. Die Patientennummer wurde durch eine laufende Nummer ersetzt. Wichtig war aus meiner Sicht, dass die Nummer nicht unmittelbar mit der Krankenakte verknüpft ist. Anderenfalls wäre hier noch eine Umschlüsselung erforderlich gewesen, da ansonsten über diese Kodiernummer Zusatzinformationen über den Patienten in Erfahrung gebracht werden könnten.

Um zusätzlich das Risiko einer Reidentifizierung zu reduzieren, habe ich im Übrigen vorgegeben, dass im Fragebogen bei den Angaben zur Person lediglich das Geburtsjahr und nicht das komplette Geburtsdatum abzufragen ist.

Die Vorgaben zum Fragebogen wurden mittlerweile auch umgesetzt.

4.8.2.2.3
Überarbeitung des Kooperationsvertrages

Ein weiteres Anliegen von mir war es, die Zusammenarbeit mit dem Universitätsklinikum besser nachvollziehen zu können. Ich habe mir daher auch noch einmal den zwischen den beiden Einrichtungen geschlossenen Vertrag vorlegen lassen.

Die daraus hervorgehenden §§ 4 und 5 enthielten über die Evaluation für die Klinik hinausgehende Zwecke. So entstand hier der Eindruck, dass die übersandten Patientendaten auch für weitere Zwecke (hier: Forschungs-, Nutzungs- und Publikationszwecke) zur Verfügung stehen.

Um zum Nachteil der Patienten Missverständnisse auszuschließen, habe ich gefordert, dass die §§ 4 und 5 des Vertrages noch einmal konkretisiert und klarer formuliert werden. Bis zum Zeitpunkt der Änderung dieser Vorschriften habe ich der Klinik vorgegeben, von einer weiteren Übermittlung von Datensätzen abzusehen.

Gemäß einer mir vorgelegten Änderungsvereinbarung wurden die unklaren Passagen aufgehoben und ganz aus dem Kooperationsvertrag herausgenommen.

4.8.3
Server einer Zahnarztpraxis im Keller eines Wohnhauses

Das Thema sichere Serverräume hat mich im letzten Jahr mehrfach beschäftigt. So erhielt ich die Anfrage, ob es auf datenschutzrechtliche Bedenken stoße, wenn der Server einer Zahnarztpraxis in einem Mehrfamilienhaus im gemeinsamen Kellerraum untergebracht ist. Ich habe die Eingabe zum Anlass genommen, mich mit den Gegebenheiten vor Ort zu beschäftigen und allgemeine Empfehlungen hieraus auszuarbeiten.

4.8.3.1
Beschwerdegegenstand

In einer Eingabe wurde mir berichtet, dass sich in einem Kellervorraum eines Wohnhauses mit mehreren Parteien der Server einer Zahnarztpraxis befinde. Die Zugangstür zu dem Kellerabteil sei über ein elektrisches Codeschloss sowie ein Sicherheitsschloss gesichert. Der Vorraum zu dem Kellerabteil könne jedoch von allen Mitbewohnern begangen werden. Auch weitere wichtige Räume wie ein Heizungs- und ein Waschraum waren nur über diesen Vorraum zu erreichen. Der Server selbst war in einem ca. 30 cm über dem Boden liegenden, fest mit der Wand montierten und verschlossenen Holzschrank untergebracht (siehe Abb.).

4.8.3.2
Rechtliche Bewertung

In Anbetracht der geschilderten örtlichen Gegebenheiten waren die Anforderungen an eine sichere Datenhaltung im Allgemeinen nicht erfüllt. Zentrale IT-Komponenten (Server, Router, Netzwerkverteiler) sind so aufzustellen, dass unbefugte Dritte keinen Zugang zu diesen Komponenten haben. Vorliegend war der Server zwar in einem Schrank eingeschlossen, dieser war aber in einem allgemein zugänglichen, nicht unter dauerhafter Beobachtung stehenden Bereich des Hauses untergebracht.

Erschwerend kommt hinzu, dass auf dem Server auch Patientendaten und damit besonders sensible Daten im Sinne des § 3 Abs. 9 BDSG abgelegt waren.

Ich musste daher beanstanden, dass es nicht auszuschließen ist, dass sich unbefugte Personen Zugang zu den Kellerräumen verschaffen können oder sich Personen unbeaufsichtigt in den Räumen aufhalten. Die Konstruktion des Schrankes bot keinen oder nur unzureichenden Schutz gegen das Aufbrechen (Diebstahl oder Manipulation des Servers).

Im Rahmen einer zwischenzeitlich erfolgten Praxisübergabe entschloss sich der neue Inhaber dazu, den Server zukünftig wieder in die Praxisräume zu verlegen. Als neuer Standort wurde ein Büroraum hinter dem Empfang vorgesehen. Da nicht auszuschließen ist, dass der Empfang in Einzelfällen unbesetzt ist, war aus meiner Sicht auch hier der Server in einem verschlossenen Schrank unterzubringen. Idealerweise konnte für den Server ein separater, ständig verschlossener Raum gefunden werden.

Erst in diesem Jahr hat eine Umfrage zum Zustand deutscher Serverräume ergeben, dass der Zustand der Serverräume „zu wünschen übrig lasse“ (siehe FAZ vom 06.10.2015, „Sichere Serverräume“). Der Vorgang zeigt, dass auch kleinere Unternehmen wie Arztpraxen ein verstärktes Augenmerk auf die datenschutzgerechte Platzierung des Servers und das entsprechende Umfeld richten müssen.

4.8.3.3
Grundsätzliches zum Umgang mit IT-Komponenten

Gerade bei sensitiven Umgebungen wie Arztpraxen und Krankenhäusern zeigen sich erhebliche Gegensätze zwischen den Anforderungen an die Praktikabilität (z. B. schneller Zugriff auf Informationen) und den Anforderungen des Datenschutzes. Deshalb möchte ich die Prüfungen in diesem Jahr zum Anlass nehmen, um einige allgemeine Informationen zu diesem Thema zu veröffentlichen.

Vor allem die sensiblen Informationen im Gesundheitsbereich erfordern einen besonderen Umgang mit IT-Systemen. Idealerweise befinden sich die zentralen IT-Komponenten in einem eigenen, verschlossenen und nicht frequentierten Raum der Praxis, zu dem nur Mitarbeiterinnen und Mitarbeiter Zugang haben. Wenn kein eigener Raum verfügbar ist, kann z. B. auch ein Lagerraum genutzt werden.

Welche weiteren Sicherungsmaßnahmen erforderlich sind, richtet sich nach den räumlichen Gegebenheiten und den Anforderungen der jeweiligen Systeme.

Beispielhaft seien hier genannt:
– Fenstersicherung/Alarmanlage (Einbruch),
– Rauchmelder (Brandgefährdung),
– Wassermelder (Wasserschäden, Löschwasser bei Brandbekämpfung) und
– besondere Maßnahmen, falls Leitungen durch den Raum führen.

Die baulichen Gegebenheiten machen oftmals eine einfache Lösung schwierig. Meine Mitarbeiter sind aber in solchen Fällen auch gerne beratend tätig.

Weitere Informationen zu Sicherungs- und Schutzmaßnahmen sind auch durch die örtliche Polizei und Feuerwehr zu erhalten.

Eine gute Übersicht über die zu beachtenden Themenbereiche zur Unterbringung von IT-Geräten liefern zudem die Maßnahmenkataloge des BSI-Grundschutzhandbuches (GSHB). Informationen zu den hier beschriebenen Themen finden sich dort im Kapitel „M 1 Infrastruktur“ sowie im Kapitel „M 4 Hard- und Software“.

4.8.3.4
Weiterführende Links

GSHB – M 1 Infrastruktur:

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M1Infrastruktur/m1infrastruktur_node.html

GSHB – M 4 Hard- und Software:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M4HardwareundSoftware/m4hardwareundsoftware_node.html

4.8.4
KV-SafeNet

Im Jahr 2015 hat die Kassenärztliche Vereinigung Hessen (KV Hessen) für ihre Mitglieder die Nutzung von KV-SafeNet für die Abrechnungen ab dem 3. Quartal verbindlich vorgeschrieben. In diesem Zusammenhang gab es Eingaben von Ärzten. Bei der Aufarbeitung der Nutzung von Sammelanschlüssen kam es zu Dissonanzen zwischen dem HDSB und der KV Hessen.

In § 295 Abs. 4 SGB V ist festgelegt, dass die Kassenärztliche Bundesvereinigung (KBV) näher regelt, wie die Abrechnung der Leistungen zu erfolgen hat. Am 08.05.2013 hat die KBV beschlossen, dass die Abrechnungsdaten nur noch elektronisch über ein von der KBV festgelegtes Verfahren vom Arzt an seine Kassenärztliche Vereinigung übermittelt werden dürfen. Als zulässige Verfahren wurden KV-SafeNet und KV-FlexNet genannt. Das KV-SafeNet ist eine hardwarebasierte Lösung, während das KV-FlexNet softwarebasiert ist.

§ 295 Abs. 4 SGB V

Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte, Einrichtungen und medizinischen Versorgungszentren haben die für die Abrechnung der Leistungen notwendigen Angaben der Kassenärztlichen Vereinigung im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern zu übermitteln. Das Nähere regelt die Kassenärztliche Bundesvereinigung.

Die KV Hessen hat diese Vorgabe im Rahmen einer Vertreterversammlung Anfang 2014 diskutiert und nach Auffassung der KV Hessen wurde beschlossen, ab dem 3. Quartal 2015 nur noch eine Abrechnung über KV-SafeNet zuzulassen. Erläuterungen dazu und Informationen über weitere Möglichkeiten des KV-SafeNet (z. B. Datenaustausch mit

gesetzlichen Unfallversicherungsträgern und Arztbriefversand) wurden den Ärzten auf regionalen Informationsveranstaltungen gegeben.

Die KV Hessen darf diese Festlegungen treffen. Der Hessische Datenschutzbeauftragte als Datenschutzaufsichtsbehörde für die KV Hessen als auch für die in Hessen niedergelassenen Ärzte hätte dann einschreiten können und müssen, wenn das Datenschutzniveau durch die Festlegung nicht mehr angemessen wäre. Das war hier nicht der Fall.

Es gab erhebliche Vorbehalte aus der Ärzteschaft, in denen u. a. die Kosten thematisiert wurden. Eine Möglichkeit, die Kosten zu reduzieren, sahen insbesondere Ärztenetze in einer gemeinsamen Nutzung der vorgeschriebenen Hardwarelösung. Die KV Hessen sah demgegenüber zwar keine Probleme bei Gemeinschaftspraxen und Praxisgemeinschaften, ansonsten lehnte sie diese sogenannten Sammelanschlüsse aber ab. In einem Rundschreiben „Digitale Vernetzung ist das Gebot der Stunde, Datenschützer erteilt Sammelanschluss klare Absage“ vom 24.07.2015 hat sie diese Auffassung noch einmal betont und dabei den Datenschutz als Kronzeugen genannt. In dem Rundschreiben wurde auch ausgeführt, dass auf Wunsch entsprechende Dokumente zur Verfügung gestellt werden. Diese Möglichkeit wurde von Ärzten genutzt und es wurde ihnen eine „gemeinsame Stellungnahme des Hessischen Datenschutzbeauftragten und der Datenschutzbeauftragten der KV Hessen“ mit Datum 24.07.2015 zugeschickt. Diese Stellungnahme war mit „Hessischer Datenschutzbeauftragter“ signiert. Von dem Rundschreiben und auch von der vorgeblichen gemeinsamen Stellungnahme erhielt ich erstmalig Kenntnis, als sich Ärzte an mich wandten, um Erläuterungen zu den Aussagen zu erhalten. Beide Dokumente waren mir vorher nicht bekannt und waren weder inhaltlich noch formal mit mir abgestimmt. Daher sah ich mich veranlasst, eine entsprechende Richtigstellung auf meiner Homepage zu veröffentlichen. Gleichzeitig forderte ich die KV Hessen auf, diese Stellungnahme nicht mehr zu versenden.

Daraufhin verschickte die KV Hessen auf Nachfrage an Ärzte eine „Stellungnahme des Hessischen Datenschutzbeauftragten zur Stellungnahme der Datenschutzbeauftragten der KV Hessen“. In dieser wird aus einer Mail zitiert, in der ich mich auf eine Anfrage der KV Hessen zu einer besonderen Fallkonstellation geäußert hatte. Diese neue Stellungnahme, wieder nicht abgestimmt, ging nicht auf die besondere Fallkonstellation, die zugrunde lag, ein und hatte zudem aus der Mail einen Absatz entfernt, ohne dass dies erkennbar war. Sie war wieder mit „Hessischer Datenschutzbeauftragter“ signiert. Auch diese Vorgehensweise habe ich gerügt und eine Unterlassung verlangt. Dem kam die

KV Hessen nach. Es folgte ein Gespräch am 03.08.2015 und Telefonate, damit Vergleichbares nicht mehr geschieht. Als abschließende Reaktion folgte am 20.08.2015 das Rundschreiben „Unser Rundschreiben vom 24.07.2015 zu KV-SafeNet“, in dem die KV Hessen den Sachverhalt klarstellte und auch ein geordnetes Vorgehen für die Beantragung und Prüfung der Zulässigkeit von Sammelanschlüssen ankündigte. Mit dieser Klarstellung habe ich den Vorgang mit den falschen Aussagen der KV Hessen für mich abgeschlossen.

4.8.5
Rechtswidriger Transfer von Diabetikerdaten in die USA?

Aufgrund verschiedener Anfragen und Beschwerden habe ich geprüft, ob personenbezogene Daten über Käufer eines Glukosemesssystems in die USA übermittelt werden, wenn sie eine im Internet kostenlos angebotene Auswertungs-Software nutzen. Anhaltspunkte für personenbezogene Datenübermittlungen habe ich nicht gewonnen. Die tatsächlich erfolgenden Datentransfers in die USA waren jedoch für die Käufer nicht hinreichend transparent. Die Informationen für die Käufer werden aufgrund meiner Forderungen präzisiert und ergänzt.

4.8.5.1
Ausgangslage

In ständig zunehmendem Maße erheben Bürgerinnen und Bürger selbst Daten über ihre Gesundheit und Fitness mittels Gesundheits-Apps und mobilen Mess- und Diagnosegeräten. Im Berichtszeitraumhabe ich diverse Anfragen und Beschwerden erhalten von Käufern des Sensors und des Lesegeräts Abbott Freestyle Libre für Diabetiker. Sie haben die Befürchtung geäußert, dass mittels der im Internet angebotenen zusätzlichen Software heimlich – entgegen den Nutzungsbedingungen – gesundheitsbezogene Daten – insbesondere Messprotokolle – in die USA übermittelt werden. Auch verschiedene Presseveröffentlichungen und Patientenforen haben diesen Verdacht aufgegriffen.

Die Käufer können Sensor und Lesegerät von der Abbott GmbH & Co. KG in Wiesbaden (im Folgenden: Abbott D) ausschließlich über deren Webseite im Direktverkauf erstehen. Der Sensor misst über einen dünnen Fühler minütlich im Unterhautfettgewebe den Glukosegehalt. Mit dem zugehörigen Lesegerät können die Werte dann mittels NFC

ausgelesen werden. Das Lesegerät bietet über ein Display erweiterte Anzeigemöglichkeiten, z. B. Verlaufskurven.

Darüber hinaus wird *auf der Webseite von Abbott D* zusätzlich als kostenloser Download eine Software von Abbott Diabetes Care Inc. (im Folgenden: Abbott USA) angeboten. Per USB-Kabel kann das Lesegerät an einen PC angeschlossen werden. Wenn die Software installiert ist, lassen sich die Messdaten vom Lesegerät auf den eigenen PC kopieren, mit der Software können diese dann vom Käufer überprüft, analysiert und ausgewertet werden.

Ich habe von Abbott D Auskunft verlangt, welche technischen und ggfs. medizinischen Informationen an Server in den USA übermittelt werden. Nach Eingang der Stellungnahme habe ich mehrere Gespräche mit Abbott D geführt, in die wegen der engen Verschränkung des Verkaufs der Messgeräte und des Angebots der zusätzlichen Software auf Vorschlag von Abbott D teilweise auch Abbott USA einbezogen wurde. Geprüft habe ich die den Käufern zur Verfügung gestellten Informationen von Abbott D und Abbott USA sowie die darin dargelegten Abläufe der Datentransfers.

Im Rahmen der Abwicklung des Kaufs werden die erforderlichen Bestelldaten – einschließlich einer individuellen Seriennummer des Geräts – von Abbott D für Produktbestellung, Bezahlung und Versand verarbeitet. Will der Käufer zusätzlich die Software von Abbott USA herunterladen, so muss er zuvor dem Lizenz- und Service-Vertrag mit Abbott USA, der auf die Freestyle Software-Datenschutzrichtlinie von Abbott USA verweist, aktiv zustimmen. Nach Zustimmung werden jedes Mal, wenn das Lesegerät mit einem Computer verbunden wird, auf dem die Software läuft und der eine aktive Internetverbindung hat, auf zwei unterschiedlichen Wegen Informationen an Abbott USA übertragen Es handelt sich dabei um die folgenden zwei Datenströme, die nicht miteinander verbunden sind:

– **Transfer 1**, um zu prüfen, ob es Updates für das verwendete System gibt. Dazu ist dem Lesegerät eine ID zugeordnet, die zufällig generiert wird (ID1). Gesundheitsdaten vom Lesegerät werden hierbei nicht übertragen.

– **Transfer 2** zum Zweck der Produktverbesserung und Entwicklung. Diese Übertragung beinhaltet Informationen über die Software- und Geräteeinstellungen sowie die Nutzung des Lesegeräts (Glukosedaten). Die Datenübertragung erfolgt unter einer per Zufallsprinzip der Software zugeordneten ID (ID2).

Nicht übertragen werden insbesondere der Name des Benutzers sowie Seriennummer von Lesegerät und Sensor. Die Daten von Transfer 1 und 2 werden auf getrennten Servern in den USA verarbeitet. Diese Trennung wird nach den mir zur Verfügung gestellten Informationen durch physische, technische und organisatorische Maßnahmen sichergestellt. Infolge der mir beschriebenen Maßnahmen von Abbott USA können die auf den beiden Wegen übertragenen Daten nicht kombiniert werden. Die bei beiden Transfers technisch bedingt mitübertragene IP-Adresse wird nur vorübergehend in den Protokollen der Webserver gespeichert und wird regelmäßig gelöscht.

4.8.5.2
Keine Übermittlung personenbezogener Käuferdaten von Abbott D in die USA

Unter Zugrundelegung der o. a. von Abbott D dargelegten Abläufe habe ich keine Anhaltspunkte dafür gewonnen, dass Abbott D Daten über Käufer des Sensors und des Lesegeräts an Abbott USA übermittelt, mit deren Hilfe Abbott USA die Nutzer der Software identifizieren könnte bzw. Abbott D dies ermöglicht.

Käufer eines Sensors und Lesegeräts haben die folgenden Optionen:

– Sensor und Lesegerät können ohne die zusätzlich angebotene Software genutzt werden.

– Die Software kann installiert und anschließend das Lesegerät nur noch dann mit dem PC verbunden werden, wenn keine Internetverbindung besteht: In dieser Konstellation werden – auch nachträglich – keine Daten in die USA übertragen.

– Die Software kann installiert und das Messgerät auch dann mit dem PC verbunden werden, wenn eine Internetverbindung besteht: Abbott USA erhält in dieser Konstellation getrennt Softwaredaten (Transfer 1) sowie Glukosedaten und Informationen zur Softwarenutzung (Transfer 2), kann diese jedoch unter Zugrundelegung der o. a. Abläufe nicht individuellen Käufern zuordnen.

Ich habe es aber als sehr problematisch angesehen, dass die Verschränkung der Angebote von Abbott D und Abbott USA und die beiden Datentransfers in die USA, die bei Nutzung der Software erfolgen können, nicht hinreichend transparent für den Nutzer sind, und eine entsprechende Präzisierung der Kundeninformationen gefordert.

Mein Anliegen in den Besprechungen war es somit, für die Nutzer der Messgeräte in Deutschland eine möglichst umfassende Transparenz über die Verarbeitung von Daten der Käufer des Sensors und des Lesegeräts sowie der Nutzer der Software herzustellen. Grundsätzlich bestand auch Konsens zwischen Abbott D und mir, dass die Transparenz für die Kunden verbessert werden soll. Die Diskussion der Details war allerdings komplex, u. a. deshalb, weil Messgerät und Software weltweit vermarktet werden und Abbott D und Abbott USA international einheitliche inhaltliche Informationen zur Verfügung stellen wollen. Die Gespräche über Formulierungen konnten daher erst im Januar 2016 abgeschlossen werden.

4.8.5.3
Transparenz für die Käufer wird verbessert

Abbott D hat mir unter Einbeziehung der Stellungnahme von Abbott USA zugesichert, dass die Informationen für die Käufer bis zum Frühjahr 2016 präzisiert und ergänzt werden.

Dies betrifft insbesondere die folgenden Aspekte:

– Abbott D hat mir schriftlich und mündlich nachvollziehbar dargelegt, dass keine personenbezogenen Daten zu den Käufern des Lesegeräts an Dritte, insbesondere nicht an Abbott USA, weitergegeben werden. Allerdings war nicht erkennbar, wo Abbott D dies den Käufern eindeutig und verbindlich zusichert. Künftig wird diese Zusicherung in die Datenschutzerklärung des Webshops (Shop Privacy Policy) aufgenommen, in dem die Kunden das Messgerät bestellen:

  „Abbott speichert Ihre Daten bezüglich der Eröffnung des Kundenkontos, der Bestellung(en) sowie der Kostenerstattung auf sicheren Servern in der EU. Ihre personenbezogenen Daten werden nicht an Länder außerhalb der EU (Drittländer, wie z. B. die USA) übermittelt."

– Lizenz- und Service-Vertrag sowie Datenschutzrichtlinie von Abbott USA
  Vor dem Hintergrund der an uns gerichteten Anfragen, die von erheblichen Verunsicherungen der Käufer zeugten, habe ich es als unverzichtbar angesehen, dass künftig den Nutzern der Software vor der Durchführung von Updates, mit denen eine Änderung der vertraglichen Grundlagen betr. das Datenschutzkonzept verbunden ist, diese Änderungen transparent und nachvollziehbar erläutert werden. Die bisher vorgesehene ausschließliche Veröffentlichung von Änderungen auf der Homepage von Abbott USA ist aus meiner Sicht nicht ausreichend.

Zugesagt wurden zwei Optionen für das künftige Verfahren:

- Im Fall von unwesentlichen Änderungen an den vertraglichen Grundlagen wird der Nutzer über ein Pop-up-Fenster informiert, das einen Link zur überarbeiteten Datenschutzrichtlinie enthält.

- Im Fall von wesentlichen Änderungen an den vertraglichen Grundlagen wird der Nutzer aufgefordert, ein Software-Update durchzuführen, und muss sich im Zuge dessen mit dem neuen Lizenz- und Service-Vertrag sowie der neuen Datenschutzrichtlinie durch Setzen eines Häkchens an entsprechender Stelle erklären.

- Es wurde mir zugesichert, dass die Darstellung des Verfahrens einschließlich des nicht personenbezogenen Datentransfers in verschiedenen Punkten in der Freestyle Software-Datenschutzrichtlinie präzisiert wird.

4.8.6
Neues Zugriffskonzept für das Krankenhausinformationssystem des Sana Klinikums Offenbach nach Datenschutzverletzungen

Nach einer Vielzahl von unberechtigten Zugriffen auf eine Krankenakte im Jahr 2014 entwickelt das Klinikum Offenbach ein neues Zugriffskonzept für sein Krankenhausinformationssystem.

4.8.6.1
Unberechtigte Zugriffe 2014

Mitte November 2014 wurde eine Studentin vor einem Fast-Food-Lokal in Offenbach niedergeschlagen. Sie wurde in das Sana Klinikum Offenbach GmbH aufgenommen. An ihrem 23. Geburtstag verstarb sie dort. Der Fall erregte erhebliches öffentliches Aufsehen. Ende Januar 2015 war in verschiedenen Presseveröffentlichungen von unberechtigten Zugriffen auf die Krankenakte zu lesen (s. z. B. Süddeutsche Zeitung vom 30.01.2015 „Etwa 90 Mitarbeiter des Klinikums Offenbach haben Medienberichten zufolge illegal die Akte ... gelesen.“).

4.8.6.1.1

Tätigwerden des Hessischen Datenschutzbeauftragten

Aufgrund der Presseveröffentlichungen haben zwei meiner Mitarbeiter bereits am 31.01.2015 vor Ort ein Gespräch geführt mit dem Geschäftsführer der Sana Klinikum Offenbach GmbH, dem Konzerndatenschutzbeauftragten der Sana Kliniken AG und der internen Datenschutzbeauftragten sowie dem verantwortlichen Techniker der Sana Klinikum Offenbach GmbH. Ziel der Gespräche war es, zu klären, wie viele Mitarbeiter tatsächlich unberechtigt auf die Krankenakte zugegriffen haben, ob die Probleme (auch) durch ein unzureichendes Konzept des Klinikums für die Zugriffe auf das Krankenhausinformationssystem (KIS) und/oder unzureichende Datensicherheitsmaßnahmen verursacht wurden und welche Maßnahmen das Klinikum bereits ergriffen hat bzw. ergreifen muss, damit solche Vorfälle soweit möglich künftig verhindert werden. Ergänzend übersandte mir das Klinikum im Februar 2015 einen schriftlichen Bericht zur Prüfung.

4.8.6.1.2

Bericht des Sana Klinikums Offenbach vom 23.02.2015 zu den erfolgten Zugriffen

Die Auswertung der Zugriffe auf die Krankenakte wurde bereits im Dezember 2014 von der Geschäftsführung initiiert. Auf der Grundlage einer Betriebsvereinbarung wurde entsprechend dem dort festgelegten Verfahren im Beisein eines Mitglieds des Betriebsrates, der Datenschutzbeauftragten und dem zuständigen IT-Mitarbeiter eine Auswertung erstellt.

Die Auswertung ergab, dass insgesamt 94 Personen (Pflegepersonal, ärztliches Personal und Verwaltungspersonal) auf die Krankenakte zugegriffen haben. Als Ergebnis der Anhörungen wurde festgestellt, dass in 31 Fällen ein Zugriff durch Mitarbeiter erfolgte, die unmittelbar in die Behandlung der Patientin involviert und daher berechtigt waren, auf diese Daten zuzugreifen. In den übrigen 63 Fällen lag eine hinreichende Begründung für den Zugriff nicht vor bzw. blieb es teilweise unklar, ob Mitarbeiter sich mit einer fremden Zugangsberechtigung Zugang zur Akte verschaffen konnten.

Das Klinikum teilte u. a. mit, dass alle 94 betroffenen Mitarbeiter bis Mitte des Jahres an der Pflichtveranstaltung „Datenschutzschulung“ teilnehmen und erneut die

Verpflichtungserklärung gemäß § 9 HDSG unterzeichnen müssen. Darüber hinaus teilte es mit, dass die Berechtigungen im KIS nochmals geprüft werden und im Rahmen der Projektgruppe zur Umsetzung der Orientierungshilfe KIS der Datenschutzbeauftragten ein neues Rollen- und Berechtigungskonzept entwickelt wird, das bis Ende 2015 vorliegen soll.

4.8.6.1.3
Rechtliche Bewertung

Positiv wurde im Rahmen der Prüfung festgestellt, dass
- generell eine Protokollierung der Lesezugriffe durchgeführt wurde,
- die Überprüfung der Zugriffsberechtigungen der Personen, die auf die Akte zugriffen, auf Eigeninitiative des Klinikums bereits vor den Presseveröffentlichungen durchgeführt wurden,
- es eine Betriebsvereinbarung gibt, die u. a. regelt, wie in Fällen eines begründeten Verdachts auf einen Straftatbestand Zugriffe auf das KIS und Auswertungen von Daten erfolgen können, und
- regelmäßig Datenschutzschulungen in der Klinik durchgeführt werden.

Problematische Aspekte und datenschutzrechtliche Forderungen:
- Das Rollen- und Berechtigungskonzept für Zugriffe auf das KIS stellt den Schutz der Patientendaten nicht hinreichend sicher und bedarf der Konkretisierung und Weiterentwicklung. Es muss auch sichergestellt werden, dass künftig Mitarbeiter nicht mehr mit fremder Kennung auf Patientendaten zugreifen können.
- Dies schließt ein angemessenes Protokollierungs- und Auswertungskonzept ein. Die aktuelle Betriebsvereinbarung sieht keine stichprobenhaften regelmäßigen Auswertungen der Zugriffe auf das KIS vor. Eine Auswertung der Protokolle fand bisher nur sehr selten statt. Derartige Auswertungen zur Überprüfung und zum Nachweis einer fehlerfreien und ordnungsgemäßen Datenverarbeitung und zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen sind jedoch rechtlich zwingend geboten (s. § 10 Abs. 2 HDSG, OH KIS Ziff. 45). Zu einem angemessenen Rollen- und Berechtigungskonzept gehört es im Rahmen der vorbeugenden Datenschutzkontrolle, 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. Dabei sollten Tools eingesetzt werden, die dies mit verhältnismäßigem Aufwand für das Klinikum ermöglichen.

4.8.6.2
Zentrale Aspekte des neues Rollen- und Berechtigungskonzepts für das KIS

4.8.6.2.1
Allgemeine Vorgaben

Bereits seit dem Jahr 2011 gibt es als Reaktion auf bundesweit festgestellte Defizite bei Krankenhausinformationssystemen als Hilfestellung für die datenschutzgerechte Ausgestaltung 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), an deren Erstellung sich auch meine Dienststelle beteiligt hat. Patienten gehen nicht davon aus und müssen nicht davon ausgehen, dass die gesamte Belegschaft eines Krankenhauses ihre Krankheitsdaten (technisch) zur Kenntnis nehmen kann. Ein Rollen- und Berechtigungskonzept muss sicherstellen, dass Mitarbeiter nur Zugang zu den Patientendaten haben, soweit und solange sie die Daten tatsächlich für ihre Aufgabenerfüllung benötigen. Unabhängig davon darf von ihnen auf die Daten nur im Einzelfall bei Bedarf zugegriffen werden.

Allerdings muss ein Rollen- und Berechtigungskonzept für ein Krankenhaus wegen der dortigen besonderen Situation (mögliche Notfälle, Überbelegung, Nachdienst, Verlegung, Konsilium) ausreichende Flexibilität ermöglichen. Von zentraler Bedeutung für den Datenschutz im Krankenhaus ist daher auch und gerade die Protokollierung der Zugriffe und eine Auswertung der Protokolle auf der Grundlage eines schriftlich verbindlich festgelegten Konzepts. Dieses Konzept sollte sowohl regelmäßige stichprobenhafte Auswertungen wie auch anlassbezogene Auswertungen im Einzelfall enthalten. Bei einem hinreichend fein differenzierten Zugriffsschutz im KIS kann die Protokollierung und auch die Auswertung der Protokolle reduziert werden. Umgekehrt steigt ihre Bedeutung in den Bereichen mit sehr weit gefassten Zugriffsberechtigungen.

4.8.6.2.2
Gegenwärtiger Stand der Umsetzung meiner Forderungen im Klinikum Offenbach

4.8.6.2.2.1
Organisatorische Maßnahmen

Die Aufarbeitung des Falles hatte ergeben, dass sich vermutlich Mitarbeiterinnen und Mitarbeiter auch mit einer fremden Zugangsberechtigung Zugang zur elektronischen Akte beschaffen konnten. Da die vom Klinikum eingesetzte Software die entsprechenden Voraussetzungen für einen schnellen Benutzerwechsel bzw. Benutzerabmeldung bietet, liegt es in der Verantwortung des einzelnen Mitarbeiters, sich bei Verlassen des PCs ordnungsgemäß abzumelden.

Um die Mitarbeiter für das Thema Datenschutz weiter zu sensibilisieren und sie mit den konkreten Anforderungen vertraut zu machen, erfolgten nach Mitteilung des Klinikums zwischenzeitlich Begehungen auf den Stationen und es wurden die entsprechenden Datenschutzschulungen intensiviert. Jeder Mitarbeiter ist verpflichtet, mindestens einmal jährlich an einer Schulung teilzunehmen.

Im Klinik-Intranet sind zudem weitere Informationen zum Datenschutz den Mitarbeitern zugänglich gemacht worden. Außerdem habe man begonnen, datenschutzrechtliche Fragen der Mitarbeiter zu sammeln und daraus für häufig auftretende Fallkonstellationen Checklisten und Handlungsempfehlungen zu erstellen.

4.8.6.2.2.2
Weiterentwicklung des Rollen- und Berechtigungskonzepts

Bereits seit 2014 beschäftigt sich im Klinikum eine Arbeitsgruppe mit der Weiterentwicklung des Rollen- und Berechtigungskonzeptes nach den Maßgaben der OH KIS.

Der vorliegende Fall zeigt, dass der Personenkreis, der technisch in der Lage war, auf die Patientenakte zuzugreifen, zu groß war. Meine Forderung nach Überprüfung der vergebenen Zugriffsberechtigungen und die von mir dargelegten Kriterien sind in die Überarbeitung des Rollen- und Berechtigungskonzeptes mit eingeflossen. Bisher konnten beispielsweise Mitarbeiter aus Organisationseinheiten, die nicht an der Behandlung des Patienten beteiligt waren, gemäß dem bestehenden Berechtigungskonzept nicht auf dessen Patientendaten zugreifen. Ein Zugriff auf Patienten außerhalb der eigenen Organisationseinheit war allerdings hilfsweise über einen „Notfallzugriff“ möglich, und zwar für einen großen Kreis von

Mitarbeiterinnen und Mitarbeitern und ohne die Notwendigkeit einer Begründung des Zugriffs (s. auch unten Ziff. 4.8.6.2.2.3).

Nach Aussage des Klinikums wurde nach Überprüfung für die Berufsgruppe „Pflege“ die Funktion „Notfallzugriff“ bereits ab dem 04.03.2015 abgestellt. Eine Prüfung, für welche ärztlichen Mitarbeiter der „Notfallzugriff“ eingeschränkt werden kann, läuft derzeit noch. Darüber hinausgehend sieht das neue Rollen- und Berechtigungskonzept jetzt auch die zeitliche Beschränkung von Zugriffsberechtigungen auf die Patientendaten vor. Einzelheiten werden nach Darstellung des Klinikums derzeit noch konkretisiert. Das Klinikum geht davon aus, dass die geplanten Änderungen bis zum Ende des 1. Quartals 2016 umgesetzt werden.

4.8.6.2.2.3
Protokollierungs- und Auswertungskonzept

Eine zentrale Forderung von mir war, dass das Protokollierungs- und Auswertungskonzept auch eine regelmäßige stichprobenhafte Prüfung der Zugriffsprotokolle auf bestimmte Auffälligkeiten hin vorsehen muss. Dabei sollen entsprechende Tools eingesetzt werden, die dies mit verhältnismäßigem Aufwand für das Klinikum ermöglichen. Von besonderer Bedeutung ist dabei z. B. die Prüfung der Verwendung des Notfallzugriffs.

Mittlerweile konnte im Sana-Konzern eine Konzernbetriebsvereinbarung zum Abschluss gebracht werden, die auch eine regelmäßige stichprobenhafte Prüfung und Auswertung der Protokolle vorsieht. Hinsichtlich des Umfangs der zu prüfenden Fälle besteht hier jedoch aus meiner Sicht noch Diskussionsbedarf.

Schwächen hinsichtlich der Protokollierung und Auswertung ergeben sich auch aus den Einschränkungen der eingesetzten KIS-Software. So ist es laut Klinikum im Krankenhausinformationssystem iMedOne gegenwärtig nicht möglich, z. B. bei Notfallzugriffen die Eingabe einer Begründung vorzusehen und die Verwendung der Notfallzugriffe gesondert auszuwerten. Tools, die die Auswertung der Protokolle auf bestimmte Auffälligkeiten hin erleichtern und somit den Aufwand des Krankenhauses im Umgang mit den Protokollierungsdaten begrenzen könnten, gibt es laut Klinikum nicht. Hier ist der KIS-Hersteller gefordert, entsprechende Lösungen anzubieten, die eine sinnvolle Protokollierung und Auswertung erlauben. Das Klinikum hat meine Forderungen an den KIS-Hersteller herangetragen.

4.8.6.2.3
Ausblick

Auch wenn der vorliegende Fall sicherlich nicht alltäglich ist, zeigt er doch, welche Bedeutung das Rollen- und Berechtigungskonzept für ein Krankenhausinformationssystem hat. Mit den bereits umgesetzten und den noch geplanten Maßnahmen ergeben sich wesentliche Verbesserungen im Rollen- und Berechtigungskonzept im Klinikum Offenbach. Dies setzt allerdings voraus, dass auch der Hersteller weitere Anpassungen in seinem Klinikinformationssystem vornimmt.

4.9
Videoüberwachung nach Bundesdatenschutzgesetz

4.9.1
Nachbarüberwachung und Kamera-Attrappen sind keine Anwendungsfälle nach BDSG

Nach wie vor erreicht mich eine hohe Anzahl von Eingaben, bei denen es um Videoüberwachung nach dem Bundesdatenschutzgesetz geht. Dennoch ist in diesem Zusammenhang eine „Trendwende" im Vergleich zu früheren Berichtszeiträumen eingetreten: Viele Videoüberwachungsanlagen sind inzwischen so installiert bzw. ausgerichtet, dass ein Verstoß gegen das Bundesdatenschutzgesetz nicht vorliegt.

Eine Vielzahl der Eingaben basiert auf klassischen Nachbarschaftsstreitigkeiten, deren „Höhepunkt" meist eine permanente Überwachung des Nachbarn ist. Ein Einschreiten liegt jedoch nicht in meinem Kompetenzbereich, wenn öffentlicher Bereich im Sinne des § 6b BDSG nicht überwacht wird.

§ 6b BDSG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

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

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

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

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

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

Unterlassungs-, Schmerzensgeld- oder Schadensersatzansprüche sind in diesen Fällen auf dem Zivilrechtsweg geltend zu machen.

Sofern im Berichtszeitraum öffentlicher Bereich im Sinne des § 6b BDSG überwacht wurde, konnte mit den Kamerabetreibern nach Darstellung der Rechtslage und ggf. Androhung eines Zwangsgeldes und/oder Ordnungswidrigkeitsverfahrens stets ein datenschutzkonformer Betrieb der Videoüberwachungsanlagen erreicht werden.

4.9.1.1

Entscheidungen des Verwaltungsgerichts Darmstadt zum Einsatz von Kamera-Attrappen, Privacy-Filter-Technik und Maßnahmen nach § 38 BDSG

In meinem 43. Tätigkeitsbericht (Ziff. 5.2.1.4) habe ich über die Videoüberwachung in Kaufhäusern und Geschäften berichtet. Die beiden in diesem Zusammenhang erwähnten Gerichtsverfahren sind inzwischen abgeschlossen. Das Verwaltungsgericht Darmstadt hat während der beiden Verfahren festgestellt, dass Kamera-Attrappen nicht in den

Anwendungsbereich des BDSG fallen, da bei der Verwendung von Kamera-Attrappen gerade **keine** personenbezogenen Daten im Sinne des § 1 Abs. 1 und 2 BDSG erhoben, verarbeitet oder genutzt werden.

§ 1 Abs. 1 und 2 BDSG

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Das Verwaltungsgericht schließt sich insoweit einer vielfach in Literatur und Rechtsprechung vertretenen Meinung an (vgl. hierzu u. a. Scholz in: Simitis, BDSG, 8. Aufl., § 6b, Rdnr. 28).

Demzufolge ist der Hessische Datenschutzbeauftragte nicht zu Maßnahmen gegen Kamera-Attrappen befugt.

Des Weiteren führt das Verwaltungsgericht Darmstadt aus, dass auch der Einsatz einer Privacy-Filter-Technik und/oder eine automatisierte Ausblendung von Bereichen, welche nicht überwacht werden dürfen (Verpixelung/Schwärzung), zu einem zulässigen Betrieb der Videoüberwachungsanlage führen können. Hierbei bedarf es jedoch einer Abwägung im konkreten Einzelfall, ob sich eine Verpixelung/Schwärzung generell dazu eignet, einen datenschutzkonformen Zustand herzustellen. Gerade bei öffentlich zugänglichen Arbeitsplätzen, wo eine Zulässigkeitsprüfung der Videoüberwachung nach § 6b BDSG und

nicht nach § 32 BDSG erfolgt, ist mit Zusatzwissen der die Aufnahmen sichtenden Personen und einer lediglich geringfügigen Verpixelung nachvollziehbar, um welche Beschäftigte es sich handelt.

Das Verwaltungsgericht führt weiterhin aus, dass Maßnahmen nach § 38 Abs. 5, S. 1 BDSG zwar auf Veränderung, aber grundsätzlich auf **Erhaltung** der Daten oder der Einrichtungen und Verfahren gerichtet sind.

§ 38 Abs. 5 BDSG

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

Eine Untersagung nach § 38 Abs. 5, S.2 BDSG als Verbot betrifft allein ein **Verhalten**, nämlich die Nutzung, nicht jedoch die Beseitigung von Hardware, sodass die Beseitigung einer Videoüberwachungsanlage von § 38 Abs. 5, S. 2 BDSG grundsätzlich nicht erfasst ist. Auch in diesem Punkt schließt sich das Gericht einer vielfach in Literatur und Rechtsprechung vertretenen Meinung an (vgl. hierzu u. a. Scholz in: Simitis, BDSG, 8. Aufl., § 6b, Rdnr. 158).

4.9.1.2
Auswirkungen dieser Entscheidungen auf die Arbeitsweise des HDSB

Eine grundsätzliche Veränderung auf die Arbeitsweise meiner Dienststelle stellen die Entscheidungen des Verwaltungsgerichts Darmstadt nicht dar. Nach wie vor gilt es zunächst festzustellen, ob es sich um eine funktionsfähige Kameraanlage oder eine Kamera-Attrappe

handelt und ob überhaupt öffentlich zugängliche Bereiche im Sinne des § 6b BDSG erfasst werden.

Im Rahmen eines aufsichtsbehördlichen Prüfungsverfahrens werden die Kamerabetreiber stets darauf hingewiesen, dass eine funktionsfähige Videoüberwachungsanlage bzw. eine Kamera-Attrappe zwar nach dem BDSG datenschutzrechtlich nicht zu beanstanden sein kann, den Betroffenen aber unter Umständen zivilrechtliche Unterlassungs-, Schmerzensgeld- oder Schadensersatzansprüche zustehen.

In diesem Zusammenhang gelangen Kamerabetreiber dann nicht selten zu der Einsicht, auch nicht in den Anwendungsbereich des BDSG fallende Kamera-Attrappen oder mit einer Verpixelung versehene Kameras so auszurichten bzw. umzubauen, dass für Dritte unzweifelhaft erkennbar ist, dass z. B. lediglich das eigene Grundstück im Fokus der Kamera(-Attrappe) steht. In einigen Fällen werden die streitgegenständlichen Anlagen freiwillig entfernt.

4.9.1.3
Zusammenfassung und Ausblick

Die Videoüberwachung wird ein „Dauerbrenner“ bleiben, die Anzahl der installierten Videoüberwachungsanlagen wird eher steigen als zurückgehen. Positiv bleibt jedoch festzustellen, dass durch die mediale Aufmerksamkeit, welche dieses Thema in den letzten Jahren erfahren hat, die Kamerabetreiber zunehmend auf datenschutzkonforme Lösungen setzen und oftmals vor Inbetriebnahme der Anlagen den HDSB einschalten.

4.10
Personalwesen

4.10.1
Datenschutzrechtliche Einwilligungen von Beschäftigten im Rahmen des Abschlusses von Arbeitsverträgen

Ist die Übermittlung von Beschäftigtendaten von einer gesetzlichen Rechtsgrundlage gedeckt, besteht keine Notwendigkeit für die Einholung einer Einwilligung. Sie wirkt in solchen Konstellationen irreführend und ist daher zu vermeiden. Aufgrund ihrer freien

Widerruflichkeit ist die Einwilligung keine taugliche Basis für Standardverfahren.

4.10.1.1
Beschwerdegegenstand

Der Betriebsrat eines Konzerns wandte sich mit der Frage an mich, ob es zulässig sei, Übermittlungen von Beschäftigtendaten an die Konzernmutter durch Einwilligungen zu legitimieren.

Das Unternehmen hatte bei Abschluss von Arbeitsverträgen diesen eine „Datenschutzerklärung“ beigefügt, in welcher die Beschäftigten ihre Einwilligung dafür zu erklären hatten, dass ihre Personaldaten an eine Zentraldatenbank der Konzernmutter übermittelt und dort verarbeitet und genutzt werden dürfen.

4.10.1.2
Rechtliche Bewertung

Das deutsche Datenschutzrecht kennt kein Konzernprivileg. Handelt es sich bei einer Datenverarbeitung weder um eine Verarbeitung innerhalb des Unternehmens, bei dem der Arbeitnehmer beschäftigt ist, noch um eine Auftragsdatenverarbeitung, ist von einer Übermittlung nach § 3 Abs. 8 BDSG auszugehen. Diese bedarf gemäß § 4 Abs. 1 BDSG einer Rechtsgrundlage oder der Einwilligung des Betroffenen.

Als Rechtsgrundlage für die Übermittlung von Beschäftigtendaten kommt zunächst § 32 Abs. 1 Satz 1 BDSG in Betracht. Diese Bestimmung setzt voraus, dass die Verarbeitung – hier also die Übermittlung der Daten der Beschäftigten eines Konzernunternehmens an die Konzernmutter – für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

Von der Erforderlichkeit einer Datenübermittlung im Konzern wird auszugehen sein, „sofern der Arbeitsvertrag einen bei Vertragsabschluss für den Betroffenen erkennbaren Konzernbezug aufweist, wenn er also ein Tätigwerden des Arbeitnehmers auch in anderen Konzernunternehmen vorsieht“ (Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ vom 11.01.2005, 3; https://www.datenschutz.hessen.de/ft-konzerndatenschutz.htm). Ein Konzernbezug, der eine Übermittlung rechtfertigt, wäre ferner auch dann gegeben, wenn bei der Einstellung des Arbeitnehmers deutlich erkennbar ist,

dass die Personaldatenverarbeitung in einem anderen Konzernunternehmen zentralisiert ist (Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ vom 11.01.2005, 3; https://www.datenschutz.hessen.de/ft-konzerndatenschutz.htm).

Auch eine Einwilligung gemäß § 4a BDSG kann Grundlage für die Übermittlung von Daten sein. Aufgrund des wirtschaftlichen Ungleichgewichts und der existentiellen Bedeutung des Beschäftigungsverhältnisses wird im Allgemeinen jedoch bezweifelt, dass auf Seiten der Beschäftigten die Einwilligung freiwillig erteilt werden kann. Dies gilt erst recht, wenn sie Voraussetzung für den Abschluss des jeweiligen Arbeitsvertrags ist.

Darüber hinaus gilt es zu bedenken, dass die Einwilligung jederzeit widerruflich ist und sie daher nur ausnahmsweise einen praktikablen Weg darstellt. Widerruft der Betroffene seine Einwilligung, hat nämlich mit dem Widerruf eine Übermittlung zu unterbleiben. Ist also die Einwilligung die einzige Rechtfertigung der Übermittlung, muss die Möglichkeit eines Widerrufs berücksichtigt und organisatorisch umgesetzt werden. Dies ist für Verfahren wie etwa die zentrale Gehaltsabrechnung wohl keine Option.

Im konkreten Fall teilte das Unternehmen mit, dass bereits im Zuge des Bewerbungsverfahrens die künftigen Mitarbeiter dahingehend informiert werden, dass die Personaldatenverarbeitung beim Mutterkonzern erfolge. Auch ergebe sich der Konzernbezug bereits aus der Organisationsstruktur des Unternehmens. Dies wurde näher ausgeführt. Die Übermittlung konnte daher auf § 32 Abs. 1 Satz 1 BDSG gestützt werden.

Da eine dennoch von den Beschäftigten eingeholte Einwilligung zu der Übermittlung ihrer Daten irreführend wäre und den Beschäftigten den unrichtigen Eindruck vermittelt, sie hätten es selbst in der Hand, ob ihre Daten an eine andere Konzerngesellschaft übermittelt werden, habe ich von einer solchen Einholung von Einwilligungen „auf Vorrat“ dringend abgeraten. Ob eine solche Einwilligung überhaupt wirksam wäre, kann bezweifelt werden, da Widerruf praktisch nicht möglich ist (Artikel 29-Datenschutzgruppe WP 187 Stellungnahme 15/2011 zur Definition von Einwilligungen, III.A.1., S. 16; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf). Geht man weiter davon aus, dass im vorliegenden Fall gemäß § 4 Abs. 1 BDSG auch auf die Folgen der Verweigerung der Einwilligung hinzuweisen ist, wären die Betroffenen auch darüber zu informieren, dass die Nichterteilung ihrer Einwilligung folgenlos bliebe. Die Datenübermittlung an die Konzernmutter würde dann auf § 32 Abs. 1 Satz 1 BDSG gestützt trotzdem rechtlich zulässig stattfinden. Spätestens diese Information macht deutlich, dass die Einholung einer Einwilligung „auf Vorrat“ in einer solchen Konstellation keinen zusätzlichen

Nutzen bringt.

Die Information der Beschäftigten gemäß § 4 Abs. 3 BDSG über die Identität der verantwortlichen Stelle, die Zwecke der Verarbeitung sowie die Kategorien der Empfänger der Daten ist hier notwendig, aber auch ausreichend. Folgerichtig hat das Unternehmen im Ergebnis darauf verzichtet, für die Übermittlung von Beschäftigtendaten Einwilligungen einzuholen. Vielmehr werden die Beschäftigten künftig in geeigneter Weise gemäß § 4 Abs. 3 BDSG über die beabsichtigte Datenübermittlung auf der Grundlage von § 32 Abs. 1 Satz 1 BDSG informiert.

5. Entwicklungen und Empfehlungen im Bereich der Informationstechnik

5.1
Windows 10 – alles umsonst?
Windows as a Service und als Cloud-gestütztes Betriebssystem

Microsoft wirbt seit 29.07.2015 bei jedem Anschalten eines PCs, der in eigener Verantwortung gewartet wird, die bestehende Betriebssystem-Installation von Windows 7 oder Windows 8.1 durch ein Upgrade auf Windows 10 kostenlos zu ersetzen. Dieses Angebot soll voraussichtlich bis zum 29.07.2016 laufen.

Microsoft bezeichnet Windows 10 als "Windows as a Service". Darunter versteht das Unternehmen, dass es im Gegensatz zu seinen Vorgänger-Versionen Windows 10 mit regelmäßigen Versions-Upgrades versorgt, die neben Sicherheits- und Fehler-Bereinigungs-Updates auch neuentwickelte Funktionen enthalten. Damit ist Windows 10 in stetiger Entwicklung. Ab Anfang November 2015 sollen alle Neugeräte mit Windows 10 als Standard-Betriebssystem verkauft werden.

Mit dem Upgrade von Windows 7 oder Windows 8.1 erhält der Nutzer oder die Nutzerin ein Cloud-gestütztes Betriebssystem. Solche Betriebssysteme – auch anderer Anbieter – versprechen eine Konvergenz der computergestützten Medien, die zu einer vielseitigeren Benutzung für jeden in bequemer Weise führen sollen. Auf jedem ähnlichen Gerät soll alles in fast immer gleicher Weise verfügbar sein, weil persönliche Informationen automatisch in die Cloud – hier von Microsoft – übertragen werden. Jeder Nutzer wird damit persönlich vor die Frage gestellt: Bequemlichkeit oder informationelle Selbstbestimmung – was ist mir wichtiger? Während der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde eine Entschließung gefasst (Ziff. 7.12: Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken), die auf diese Datenschutz-Risiken hinweist.

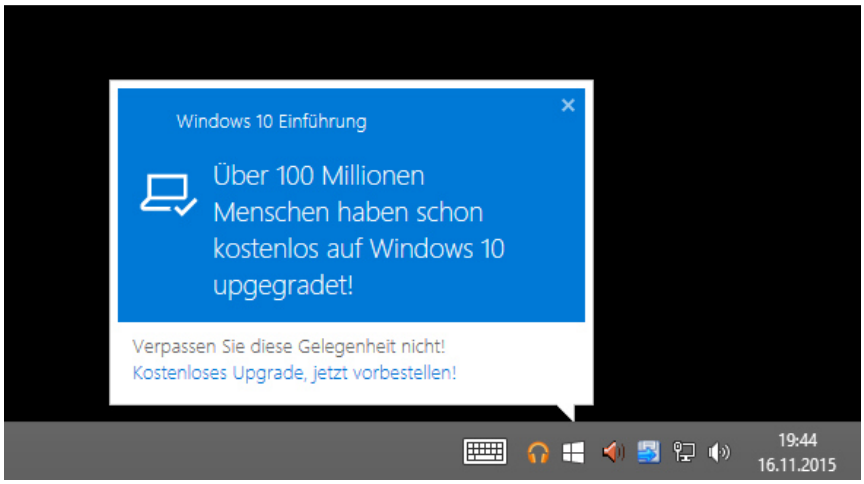

Abbildung (16.11.2015): „Get Windows 10 Programm“ (GWX) im Infobereich neben der Uhr

5.1.1
Datenschutz und Cookies

Mit der jetzt begonnenen Einführung von Windows 10 hat Microsoft seine Datenschutz-Erklärung unter dem Titel „Datenschutz und Cookies“ vereinheitlicht. Sie bezieht sich zunächst auf diverse Produkte, die der Kunde erwerben kann. Die Datenschutz-Erklärung als entsprechendes, gesamtes Dokument erhalten Nutzende im Web. Innerhalb dieses Dokuments zum Datenschutz bleiben jedoch viele Formulierungen sehr vage.

Eine produktbezogene und verschieden ausgestaltete Einwilligung zu der Datenschutz-Erklärung wird im Installationsprozess schrittweise online durchgeführt. Wer sich für die Express-Installation entscheidet, erhält einen reduzierten Fragenkatalog zum Datenschutz. Damit kommt es bei der Erst-Installation wesentlich darauf an, welche Vorgangsweise gewählt wird und ob (und wie viele!) nutzerspezifische Daten im Rahmen des Setups sofort an Microsoft übertragen werden. Zu diesen personenbezogenen Daten gehören, wenn keine einschränkenden Einstellungen vorgenommen werden, der Name des Nutzers oder der Nutzerin, Adresse, Alter, Geschlecht und Telefonnummer und der jeweilige Standort des Geräts, sobald dieses mit dem Internet verbunden ist. Des Weiteren werden mit der Internet-Verbindung auch die aufgerufenen Web-Seiten an Microsoft übertragen. Nach der Installation hat der Nutzer – an mehreren Stellen im System verteilt – die Möglichkeit einige Einstellungen vorzunehmen, die die Anzahl der an Microsoft übermittelten Daten reduziert.

Insgesamt ist mit diesem Verfahren eine Opt-Out-Lösung realisiert, wobei der Nutzer oder die Nutzerin ggf. auch Verluste in der Bedienbarkeit und Funktion von Windows 10 hinnehmen muss. Datenschutzfreundlich wäre ein Opt-In, so dass durch den Nutzer

bestimmt werden kann, für welchen konkreten Zweck er einer Datenübermittlung zustimmt und damit akzeptiert, dass damit ggf. auch eine Funktion oder eine integrierte Anwendung ein- oder ausgeschaltet wird. Zudem müsste sichergestellt sein, dass ein solches Ausschalten auch tatsächlich eine weitere Datenübertragung an Microsoft unterbindet.

5.1.2
Permanenter Internetzugang

Ohne einen permanenten Internetzugang funktioniert in der neuen Windows-Version so gut wie nichts, da Sicherheits- und Funktions-Updates sowie Funktions-Upgrades ohne weiteres Zutun automatisch nach der Freigabe durch Microsoft eingespielt werden. Das geschieht beim heutigen Entwicklungsstand fast täglich. Die bisher vorhandene umfangreiche Steuerung über die Einstellmöglichkeiten der Systemsteuerungs-Komponente „Windows Update“ ist hingegen ersatzlos weggefallen. Einzig Firmenkunden haben noch eingeschränkt die Möglichkeit, Funktions-Updates zu beeinflussen: In der Enterprise-Version können diese für eine gewisse Zeit hinausgeschoben werden, Windows 10 LTSB (Long Time Service Branch) ist eine Version für kritische Infrastrukturen, für die nur Sicherheits-, jedoch keine Funktions-Aktualisierungen angeboten werden.

Diejenigen, die ein Gerät mit verwalteter Windows 10-Installation besitzen, werden somit von Microsoft gemanagt. Diese Situation bleibt insbesondere auch deshalb kritisch zu bewerten, weil die Frage offen ist, was zum Ende des Jahres 2016 durch Upgrade verteilte Lizenzen wird: Welchem Lizenz- und Kostenmodell liefert sich der Nutzer aus?

5.1.3
Eigene Evaluationen

Im Testlabor des Hessischen Datenschutzbeauftragten wurde Windows 10 wiederholt über Upgrade und andere Installationsverfahren getestet, um mehr über die Datenflüsse zu erfahren. Die vorgestellten Betrachtungen müssen somit eine Momentaufnahme sein, die allerdings zeigen, dass es notwendig sein wird, die Entwicklungen stetig und wachsam zu verfolgen. Eine entsprechende fortgeschriebene Dokumentation dieser Ergebnisse findet sich auf meiner Homepage im Bereich „Fachthemen“, „IT-Systeme und Anwendungen“.

Zu erwarten ist, dass die schon einmal vor Jahren geführte Krypto-Debatte erneut aufkommen wird: Wenn keine vollständige Entkopplung der Datenflüsse möglich zu sein scheint, ohne dass die Funktionalität fast bis zur Untauglichkeit eingeschränkt wird, dann gilt es die Fragen nach Vertraulichkeit und Integrität erneut zu beantworten.

5.2
Verfahrensverzeichnisse für Systeme aus den Bereichen des Unified Messaging und der Computer Telefonie Integration

Moderne Kommunikationsverfahren aus den Bereichen UM und CTI können nicht als Teil „einfacher" Telekommunikationsanlagen angesehen werden. Ihre notwendigen Schnittstellen zu TK-Anlagen und der IT-Umgebung einer datenverarbeitenden Stelle sowie die gespeicherten Daten von externen Kommunikationspartnern und insbesondere der Mitarbeiter machen ein Verfahrensverzeichnis nach § 6 HDSG erforderlich.

Im abgelaufenen Kalenderjahr war für zwei Anfragen aus dem Bereich der Landesverwaltung zu prüfen, ob die Einordnung der betreffenden Systeme als Standardverfahren im Sinne des Erlasses des HMDIS zu §§ 6 und 15 HDSG (StAnz. 17/1999 S. 1226) zulässig bzw. verhältnismäßig ist.

Der Erlass hatte in der Zeit seiner Entwicklung u. a. zum Ziel, den Verfahrensbegriff umfassend abzugrenzen. Damit wurde beispielsweise geregelt, dass nicht jede lokale Textverarbeitungssoftware, die geeignet ist Adressen und persönliche Einzeldaten Betroffener zu verarbeiten, als Verfahren erfasst werden muss. Damals ist man davon ausgegangen, dass auch einfache Telefonanlagen, die nur allgemein der Kommunikation und keinem speziellen Verarbeitungszweck dienen, nach einer Vorabkontrolle als Standardverfahren ohne Verfahrensverzeichnis eingestuft werden können. Doch die Entwicklung von TK-Anlagen und deren immer komplexere Einbindung in die IT-Strukturen von datenverarbeitenden Stellen durch ergänzende Verfahren machen eine Neubewertung dieser Frage erforderlich.

Bei den betroffenen Systemen handelt es sich zum einen um einen zentralen Fax-, SMS- und Voicebox-Server der Landesverwaltung, zum anderen um eine CTI-Lösung einer staatlichen Bühne. In beiden Fällen sind die Systeme mit Schnittstellen an die TK-Anlage bzw. an den E-Mail-Transport-Server gekoppelt. Für die Zuordnung der Nachrichten bzw. der

dazu gehörenden Meta-Informationen werden in diesen Systemen zusätzlich immer Personal-Daten aus anderen Verfahren gebraucht oder zusätzlich generiert.

Problematisch ist in beiden Anwendungsfällen, dass die Komfortmerkmale der zusätzlichen Technik an Arbeitsplätzen mit besonderen Vertrauensstellungen, wie z. B. der Frauenbeauftragten oder der Personalratsmitglieder, nur eingeschränkt oder ggfs. gar nicht zu kritischen Speicherungen von Verbindungsdaten führen dürfen.

Für die Transparenz der Verfahren gegenüber den Betroffenen ist daher eine Einordnung als Standardverfahren nicht verhältnismäßig, eine Erfassung als Verfahrensverzeichnis der jeweiligen datenverarbeitenden Stelle notwendig.

Ich werde diese Entscheidung zum Maßstab für alle zukünftig vorliegenden Anfragen machen. In Fällen, in denen es sich technisch und organisatorisch anbietet, kann ggf. eine Ergänzung eines vorhandenen Verfahrensverzeichnisses vorgenommen werden.

5.3
Datenschutz bei Smart-TV-Angeboten

Fast alle heute erhältlichen Fernsehgeräte sind sog. Smart-TV, die mit dem Internet verbunden werden können und so zusätzlich zum Fernsehen diverse weitere Dienste ermöglichen. Während herkömmliche Fernseher nur passiv das Rundfunksignal empfangen konnten, senden Smart-TV auch selbst Daten an die Anbieter der verschiedenen Dienste. Da diese Daten teilweise Rückschlüsse auf den Fernsehzuschauer ermöglichen, müssen die Anbieter von Smart-TV-Diensten die Anforderungen des Datenschutzrechts beachten.

Fernseher sind mittlerweile, wie viele andere Geräte auch, dank der Verbindung mit dem Internet „smart“ geworden und bieten viel mehr Funktionen als nur den Empfang des klassischen Fernsehprogramms. So können mit einem Smart-TV beispielsweise Hintergrundinformationen zum Programm abgerufen, Videos und Musik gestreamt und diverse Apps genutzt werden. Die verschiedenen Smart-TV-Dienste werden von unterschiedlichen Anbietern bereitgestellt, zumeist sind dies die Gerätehersteller, Fernsehsender und Anbieter von Apps.

Die Nutzung von internetbasierten Diensten erfordert aber immer auch den Austausch von Daten zwischen dem Anbieter des jeweiligen Dienstes und dem vom Nutzer verwendeten

Gerät. Schon anhand der Daten, die für die Verbindung mit dem Internet technisch erforderlich sind (wie z. B. der IP-Adresse des Smart-TV), können von den Anbietern von Smart-TV-Diensten unter Umständen Rückschlüsse auf das Verhalten des Nutzers gezogen werden. Zudem besteht die Gefahr, dass der Fernseher ohne Wissen und Einverständnis des Zuschauers bestimmte Informationen an den Hersteller, an Rundfunksender oder an andere Dritte sendet. Insbesondere Informationen über die Fernsehgewohnheiten einzelner Zuschauer sind für alle werbetreibenden Unternehmen äußerst interessant, da anhand solcher Daten z. B. personalisierte Werbung platziert werden kann.

Um den verschiedenen datenschutzrechtlichen Problemen bei der Nutzung von Smart-TV zu begegnen, haben sich die deutschen Datenschutzaufsichtsbehörden im Berichtszeitraum gemeinsam des Themas angenommen. So wurde zum einen eine gemeinsame Orientierungshilfe erarbeitet, die sich an alle Unternehmen richtet, die Smart-TV-Dienste anbieten. Darin finden sich Hinweise, wie die jeweiligen Angebote datenschutzgerecht gestaltet werden können. Zum anderen haben mehrere Aufsichtsbehörden, darunter auch meine Dienststelle, eine technische Prüfung von TV-Geräten der wichtigsten auf dem deutschen Markt vertretenen Hersteller vorgenommen. Dabei wurde untersucht, welche Datenflüsse bei der Nutzung der Geräte entstehen.

Im Rahmen der technischen Prüfung, die in Zusammenarbeit mit dem Bayerischen Landesamt für Datenschutzaufsicht durchgeführt wurde, wurden u. a. Smart-TV-Geräte zweier international führender Elektronikkonzerne geprüft, die einen Geschäftssitz in Hessen haben und daher meiner Aufsicht unterliegen. In verschiedenen Prüfszenarien wurde untersucht, welche Daten bei der Nutzung bestimmter Funktionen an welche Stellen übermittelt werden. Besonderes Augenmerk wurde dabei darauf gelegt herauszufinden, ob es auch mit einem mit dem Internet verbundenen Smart-TV möglich ist, wie mit einem herkömmlichen Fernseher anonym fernzusehen.

Bei der Prüfung stellte sich heraus, dass manche Daten, die vom Fernseher an die jeweiligen Diensteanbieter übermittelt werden, Rückschlüsse auf die Person des Fernsehzuschauers und auf dessen Nutzungsgewohnheiten zuließen. Allerdings sind viele der von den Geräten übertragenen Daten für die Erbringung der jeweils genutzten Dienste erforderlich. In diesem Rahmen ist die Datenverarbeitung in der Regel zulässig. Es wurden jedoch auch einzelne Datenflüsse festgestellt, deren Zulässigkeit zumindest fraglich erschien. Im Rahmen der derzeit noch andauernden Prozesse werde ich darauf hinwirken, dass die Hersteller mittels der Smart-TV-Geräte nur im zulässigen Umfang Daten erheben.

Besondere Beachtung wurde sowohl der technischen Geräteprüfung als auch der Erstellung der Orientierungshilfe, dem sog. Hybrid Broadcast Broadband TV (HbbTV), geschenkt. Der HbbTV-Dienst ermöglicht ein internetbasiertes Zusatzangebot der TV-Sender, das während des Empfangs des jeweiligen Senders vom Zuschauer aufgerufen werden kann. Dazu sendet der Rundfunksender zusammen mit dem digitalen Fernsehsignal (z. B. über Kabel oder Satellit) die URL einer Webseite, anhand der sich der Smart-TV automatisch über das Internet mit dem Server des Fernsehsenders verbindet. Die dann meist rechts unten im Fernsehbild eingeblendete Applikation ermöglicht über das Drücken des roten Knopfes auf der Fernbedienung („Red Button“) den Zugriff auf die Onlinedienste des Fernsehsenders (z. B. weitere Informationen zu Sendungen oder Mediatheken).

Die derzeitige technische Ausgestaltung des HbbTV-Dienstes ermöglicht es, dass die Rundfunksender Informationen über die Fernsehgewohnheiten der einzelnen Zuschauer gewinnen können, auch ohne dass diese den Dienst selbst in Anspruch nehmen. Vielmehr können bestimmte Informationen allein dadurch gesammelt werden, dass der Zuschauer einen Fernsehsender einschaltet bzw. zu anderen Sendern umschaltet. Da der Dienst auf den meisten Smart-TV per Werkseinstellung standardmäßig aktiviert ist, wird auf diese Weise eine Erhebung von Daten möglich, die den meisten Smart-TV-Nutzern nicht einmal bewusst sein dürfte. Aus diesem Grund wurden die deutschen Fernsehsender von den Datenschutzaufsichtsbehörden der Bundesländer dazu aufgefordert, ihre HbbTV-Dienste so zu überarbeiten bzw. einzusetzen, dass sie den datenschutzrechtlichen Anforderungen zukünftig entsprechen.

Damit der Beachtung des Datenschutzrechts bei Smart-TV-Angeboten größere Bedeutung geschenkt wird, werde ich weiterhin auf die in Hessen ansässigen Anbieter einwirken, damit diese ihre Dienste und Geräte datenschutzgerecht gestalten. Einen Überblick über die dazu erforderlichen Anforderungen können sich alle Anbieter von Smart-TV-Diensten anhand der auf meiner Homepage im Bereich „Fachthemen“, „Fernsehen und Rundfunk“ veröffentlichten „Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste“ verschaffen.

5.4
Smart-TV – ein Sicherheitsrisiko im Heimnetzwerk

Jedes Gerät mit IP-Adresse in einem privaten Netz, das mit dem Internet kommuniziert, kann durch Hacker angegriffen werden. Der Smart-TV ist in diesem Punkt keine Ausnahme, sondern im Gegenteil ein eher reizvolles Ziel.

Im Berichtsjahr haben die Medien über mehrere Fälle berichtet, in denen Smart-TV Ziel von Angriffen und Manipulationen wurden.

Die Hersteller legen großen Wert auf Bedienerfreundlichkeit und stellen den Nutzern komfortable Benutzeroberflächen, die ständig optimiert werden, zur Verfügung. Die Geräte selbst sammeln daher Informationen, um die Optimierung und Akzeptanz der Produkte zu verbessern. Ob und inwieweit dies datenschutzrechtlich zulässig ist, wird derzeit noch geprüft (s. Ziff. 5.3).

Auf die Aspekte der IT-Sicherheit sind die Betriebs- und Kommunikationssysteme der Smart-TV nicht vorrangig eingerichtet. Sie können daher für Hacker, die ein Small-Office-Home-Office-Netz attackieren möchten, ein interessantes Zielobjekt im jeweiligen Netz sein. Ist der „Fernseher“ erst mal „gekapert“ bzw. übernommen, lässt sich von dort das gesamte Netzwerk weiter ausforschen.

Für die Hersteller der Geräte wird es zukünftig notwendig, wie dies bereits für die Anbieter von Betriebssystemen und Software, die mit dem Internet kommunizieren (Browser, streaming-client ...), heute üblich ist, für alle Gerätegenerationen regelmäßig sog. Firm-Updates bereitzustellen, wenn Schwachstellen an den verbauten Hard- und Softwarekomponenten bekannt werden.

Insbesondere für ältere Gerätegenerationen, die möglicherweise noch in kleinen Stückzahlen in den Haushalten zu finden sind, wird dieser Update-Service zu einer aufwändigen und teuren Angelegenheit. Noch schwieriger wird die Situation, wenn einzelne Hersteller nicht mehr im Wettbewerb stehen und es für deren Geräte keine Updates mehr gibt. Hier stellt sich nun die Frage: Wie lassen sich die betroffenen Geräte weiterhin sicher im privaten Netz betreiben?

Das Smart-TV-Gerät ist wegen seiner schon heute hohen Marktdurchdringung das bekannteste Beispiel aus dem Teilbereich der Unterhaltungselektronik, welches stellvertretend für die Probleme der Smart-Home-Entwicklung in den Haushalten steht. Ein Gerätehersteller, der bereits eine Fülle smarter Geräte und Komponenten für den Haushalt anbietet, hat angekündigt, bei seinen Smart-Home-Angeboten das Smart-TV zur Steuerzentrale zu machen.

Er steht damit in Konkurrenz zu Smart-Home-Konzepten aus anderen Marktsegmenten. Hier wären beispielsweise die Energieversorger oder die Router-Hersteller zu nennen. Alle Anbieter sind aufgefordert, durch entsprechende Konzepte die Sicherheit ihrer Produkte und Lösungen dauerhaft zu gewährleisten.

Der Verbraucher muss am Ende entscheiden, welchem Angebot er sein privates Netzwerk und nicht nur seinen TV-Konsum anvertrauen will.

5.5
Apps und Auftragsdatenverarbeitung

Auch wenn Kommunen personenbezogene Daten mittels App erheben, ist ein Vertrag nach § 4 HDSG erforderlich, sofern Serverkomponenten von einem Dienstleister betrieben werden.

Dem anhaltenden Boom von Mobil-Geräten wie Smartphones und Tablet-Computern wollen sich auch öffentliche Einrichtungen nicht entziehen. Im Laufe des letzten Jahres habe ich mit Interesse beobachtet, dass jetzt auch Gemeinden zunehmend als App-Anbieter auftreten und Apps in Auftrag geben, insbesondere für die Bereiche Tourismus und Abfallwirtschaft. Meine Aufmerksamkeit wurde durch eine Eingabe geweckt, die mich auf eine App einer hessischen Gemeinde hinwies, welche zunächst nicht datenschutzgerecht ausgestaltet war. Sie verarbeitet folgende personenbezogenen Daten ihrer Nutzer:

– Name
– E-Mail-Adresse
– Telefonnummer
– Standort
– Fotografien.

Die personenbezogenen Daten werden für folgende Zwecke benötigt:

– Nachrichten/Neuigkeiten aus der Gemeinde
– Abfallkalender (insbesondere Übersicht über die Abholtermine)
– Interaktive Karte mit Sehenswürdigkeiten
– Liste von Mitarbeitern der Gemeinde mit Bild, Anschrift, Telefon, E-Mail und Sprechzeiten
– Schadensmelder: Mängel und Missstände an die Gemeinde melden (Name, E-Mail/Telefonnummer, Standort, Beschädigung, Fotografien)

– Allgemeine Gemeinde-Information.

Bei Entwicklung und Betrieb dieser Programme für Mobil-Geräte sind nicht nur die für „klassische“ Programme bekannten Themen zu beachten, sondern es gilt neue Punkte einzubeziehen:

5.5.1
Auftragsdatenverarbeitung

In der Regel benötigen Apps eine Serverkomponente, um ihre Funktion zu erfüllen. Diese wird oft von Dienstleistern betrieben, bei besagter App durch den Hersteller. Wenn eine Gemeinde mittels einer solchen App personenbezogene Daten erfasst und nutzt, werden diese Daten durch den Dienstleister im Auftrag, wie auch oft bei „klassischen“ Programmen, verarbeitet. Dies hat zur Folge, dass ein Vertrag nach § 4 HDSG abgeschlossen werden muss, der die Rechte und Pflichten von Auftraggeber und Auftragnehmer festlegt. Im vorliegenden Fall hatte die Gemeinde allerdings nicht berücksichtigt, dass Name, E-Mail-Adresse, Telefonnummer, Standort und Bilder personenbezogene Daten sind; nach Einschätzung der Gemeinde seien diese Daten einfach „nicht brisant“.

Nach meiner Erläuterung, was personenbezogene Daten sind (§ 2 HDSG),

> § 2 Abs. 1 HDSG
>
> Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

wurde mit dem Betreiber ein Vertrag nach § 4 HDSG abgeschlossen.

> § 4 HDSG
>
> (1) Die datenverarbeitende Stelle bleibt für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie für die Erfüllung ihrer sich aus § 8 ergebenden Pflichten auch dann verantwortlich, wenn personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz

oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

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

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

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

5.5.2
Datenschutzerklärung

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

§ 13 Abs. 1 TMG

Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten (...) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist.

Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Die besagte App hatte anfangs keine Datenschutzerklärung. Jetzt werden den Nutzern ausreichende Datenschutzinformationen zur Verfügung gestellt. Um dies zu gewährleisten, ist es unbedingt erforderlich, dass App-Anbieter Transparenz für die App-Nutzer herstellen. Siehe hierzu mein Hinweis „Aufgabe für App-Anbieter - Transparenz für Android App-Nutzer herstellen!“ auf meiner Homepage im Bereich „Fachthemen/Mobile Geräte“.

5.5.3
Datensicherheit

Grundsätzlich sollten öffentliche Stellen bei der Beauftragung einer App den Auftragnehmer dazu verpflichten, die Empfehlungen der „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ des Düsseldorfer Kreises (Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) zu beachten, welche sich auf meiner Homepage im Bereich „Fachthemen / Mobile Geräte“ befindet.

Bei der Prüfung der vorliegenden App ergaben sich keine Anhaltspunkte, dass die Datensicherheit gefährdet ist.

5.6
Umsetzung der sog. Cookie-Richtlinie in deutsches Recht

Die Datenschutzbeauftragten des Bundes und der Länder haben im Frühjahr 2015 einen erneuten Versuch unternommen, Bundesregierung und Bundesgesetzgeber dazu zu bringen, die europarechtliche Vorgabe, wonach Diensteanbieter Cookies und andere Technologien zur Verfolgung des Nutzerverhaltens im Internet nur mit informierter Einwilligung der Nutzer einsetzen dürfen, in nationales Recht umzusetzen (Entschließung vom 05.02.2015, s. Ziff. 7.1). Bislang gibt es jedoch keine Anzeichen, dass die Bemühungen diesmal von Erfolg gekrönt sein könnten.

5.6.1
Cookies

Cookies („Plätzchen“) sind kurze Texte, die beim Besuch einer Website vom Server des Webseitenbetreibers auf dem Rechner des Nutzers im Browser gespeichert werden. Cookies können aber auch von einem anderen Diensteanbieter als dem Betreiber der besuchten Webseite auf dem Computer des Nutzers installiert werden, sogenannte Drittanbieter-Cookies. Wenn z. B. auf einer Webseite die altgediente „Gefällt mir“-Schaltfläche oder die mittlerweile übliche „Teilen“-Schaltfläche von Facebook verwendet werden, setzen diese auf der Webseite eingebundenen sogenannten „soziale Plug-ins“ ein Drittanbieter-Cookie, in diesem Fall von Facebook. Das Gleiche gilt für Werbebanner, die von Dritten auf der Webseite platziert werden. Bei jedem späteren Besuch der Seite sendet der Rechner des Nutzers die Cookie-Informationen an den Webseitenserver bzw. an den Drittanbieter.

Cookies können beliebige Informationen enthalten, wie z. B. die vom Nutzer bevorzugte Sprache oder andere persönliche Seiteneinstellungen, Anmeldeinformationen, ID-Nummern, Klarnamen, Postanschriften oder E-Mail-Adressen.

Im Hinblick auf Funktion und Lebensdauer lassen sich zwei Arten von Cookies unterscheiden: Session Cookies haben keine feste Speicherdauer. Sie werden gelöscht, wenn der Browser nach dem Surfen im Internet (der Session) geschlossen wird. Daneben gibt es dauerhafte (persistente) Cookies, die für einen bestimmten Zeitraum gespeichert bleiben. Das können Monate oder auch Jahre sein. Der von Amazon auf dem Rechner des Besuchers hinterlegte Cookie „ubid-acbde“ bleibt beispielsweise 20 Jahre gültig (s. Abb. 1). Ohne Cookies wäre die Webnutzung häufig sehr unkomfortabel. Die Plätzchen erleichtern die Nutzung der Webseiten, indem der Webserver Präferenzen des Nutzers erkennt. Virtuelle Warenkörbe in Onlineshops sind erst durch Cookies möglich. Bei Abbrüchen von Verbindungen zum Server lassen sich mittels Cookies Webanwendungen dort fortsetzen, wo sie abgebrochen wurden, sie müssen also nicht komplett wiederholt werden.

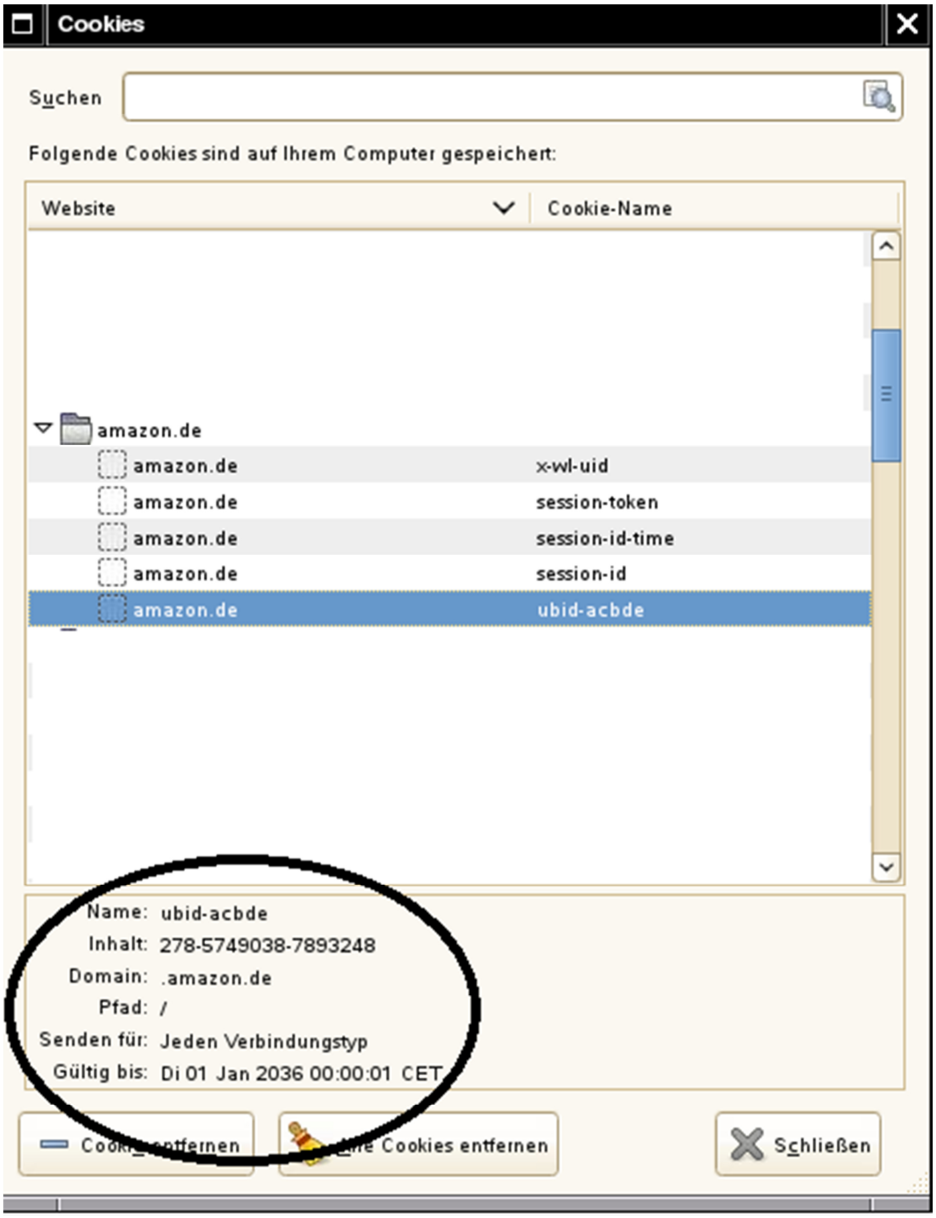

Abb. 1

5.6.2
Risiken

Allerdings bergen Cookies auch Risiken für den Nutzer. Die in ihnen gespeicherten Identifikationsmerkmale machen den Nutzer über mehrere Seitenaufrufe wiedererkennbar, sodass sich Profile über das Surfverhalten des Nutzers erstellen lassen. Ein Webseitenbetreiber, z. B. ein Onlineshop, kann daher über einen langen Zeitraum das Verhalten des Nutzers protokollieren. Drittanbieter, die sogenannte „tracking cookies“ verwenden (z. B. Agenturen, die über Werbebanner auf vielen unterschiedlichen Seiten Cookies setzen), können die Besuche eines Nutzers auf allen diesen Seiten nachvollziehen

und verknüpfen und so serverübergreifend den Benutzer verfolgen (tracken). Bei den Standardeinstellungen der Browser bemerkt der Nutzer nicht, wenn Cookies auf seinem Rechner gesetzt werden oder Daten an den Webseitenbetreiber übermitteln.

5.6.3
Cookie-Richtlinie der EU

Die EU hat deshalb 2009 in der Datenschutzrichtlinie für die elektronische Kommunikation, auch E-Privacy-Richtlinie genannt (Richtlinie 2009/136/EG vom 25.11.2009 zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation [ABl. L 337 vom 18.12.2009, S. 11]), in Art. 5 Abs. 3 vorgeschrieben, dass Cookies nur gesetzt werden dürfen, wenn der Surfer nach vorheriger Information seine Einwilligung gegeben hat (daher auch die Bezeichnung „Cookie-Richtlinie“).

Art. 5 Abs. 3 Richtlinie 2009/136/EG

Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Unproblematisch sind demnach die Session Cookies, die das Navigieren auf Webseiten erleichtern und nach Schließen des Browsers gelöscht werden. Von der Richtlinie erfasst werden lediglich Cookies, die der Verfolgung des Nutzerverhaltens, sei es auf der Webseite oder webseitenübergreifend, dienen.

5.6.4
Umsetzung

EU-Richtlinien gelten jedoch nicht unmittelbar in den Mitgliedstaaten, sondern müssen von diesen in nationales Recht umgesetzt werden. Im Fall der Cookie-Richtlinie hat die EU den Mitgliedstaaten hierfür eine Frist bis 25.05.2011 gesetzt (Art. 15a Abs. 1 der Richtlinie). Nach Ansicht der Aufsichtsbehörden ist die Umsetzung der Richtlinie in Deutschland bislang unterblieben, auch wenn die Bundesregierung und mit ihr die EU-Kommission das anders sehen. Bereits mit Beschluss des Düsseldorfer Kreises vom 24./25.11.2010 haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich auf das Regelungsdefizit hingewiesen. Das Bundeswirtschaftsministerium und – gestützt auf eine Stellungnahme des Ministeriums – auch die EU-Kommission sind der Meinung, dass die Vorgaben des Art. 5 Abs. 3 der Richtlinie bereits im Telemediengesetz enthalten seien. Dem ist jedoch nicht so. Das Erstellen von Nutzungsprofilen ist in § 15 Abs. 3 TMG geregelt. Die Vorschrift verpflichtet die Diensteanbieter lediglich, die Nutzer zu informieren und ihnen ein Widerspruchsrecht einzuräumen. Dies gilt auch, wenn Nutzungsprofile mittels Cookies erstellt werden. Eine Einwilligung, wie in der Richtlinie gefordert, verlangt das TMG nicht. Im Gegensatz zur Richtlinie setzt § 15 Abs. 3 TMG auch nicht bei der Speicherung von Informationen auf dem Endgerät des Nutzers an, sondern erst bei der Verwendung dieser Daten für Nutzungsprofile.

§ 15 Abs. 3 TMG

Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Der Bundesgesetzgeber sollte sinnvollerweise auch gleich mitregeln, wann von einer wirksamen Einwilligung des Nutzers ausgegangen werden kann. Art. 5 Abs. 3 der Datenschutzrichtlinie für die elektronische Kommunikation lässt einen weiten Interpretationsspielraum. Dementsprechend vielfältig sind in den Mitgliedstaaten der EU die Lösungen. Sie reichen von der Notwendigkeit einer ausdrücklich erklärten Einwilligung über eine Einwilligung durch die Browsereinstellung (wofür auch Erwägungsgrund 66 der Richtlinie spricht), einer konkludenten Einwilligung bis zur Einräumung einer Widerspruchsmöglichkeit. Eine ausdrückliche Einwilligung dürfte angesichts der Vielzahl der Cookies kaum praktikabel sein. Die britische Datenschutzaufsichtsbehörde (ICO) hat diese

Praxis nach relativ kurzer Zeit aufgegeben. Mit dem Thema Einwilligung für Cookies haben sich die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten in der Artikel 29-Datenschutzgruppe mehrfach beschäftigt (WP 171 vom 22.06.2010, WP 188 vom 08.12.2011, WP 194 vom 07.06.2012, WP 208 vom 02.10.2013, WP 224 vom 25.11.2014). Im letztgenannten Dokument kommt die Artikel 29-Datenschutzgruppe zu dem Ergebnis, dass auch digitale Geräte-Fingerabdrücke (device fingerprints) unter den Anwendungsbereich des Art. 5 Abs. 3 fallen. Mit dieser Technik lässt sich aufgrund von Daten über Betriebssystem, Browserversion und Browsereinstellungen oder Bildschirmeinstellungen usw. der Rechner identifizieren und unter Umständen das Surfverhalten des Nutzers verfolgen, ohne dass Cookies gesetzt werden.

5.6.5
Folgen

Da auch die Bedingungen, die der EuGH für eine unmittelbare Geltung von Richtlinienvorschriften formuliert hat, im Hinblick auf Art. 5 Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation nicht erfüllt sind, führt die Untätigkeit des Bundesgesetzgebers dazu, dass den Aufsichtsbehörden in Deutschland die Hände gebunden sind. Solange eine Umsetzung in deutsches Recht unterbleibt, sind die Aufsichtsbehörden an der Durchsetzung des Art. 5 Abs. 3 gehindert. Darauf haben die Datenschutzbeauftragten Bundesregierung und Bundesgesetzgeber mit ihrem Beschluss vom 05.02.2015 nochmals eindringlich hingewiesen.

5.6.6
Kontrollmöglichkeiten der Nutzer

Entschärft wird das Problem dadurch, dass inzwischen die meisten Webbrowser den Nutzern die Möglichkeit zur Kontrolle von Cookies bieten.

Unabhängig von der Umsetzung der Richtlinie sind Webseitenbetreiber nach geltendem nationalem Recht verpflichtet, den Nutzer eindeutig und klar verständlich über den Zweck der Speicherung von Cookies und der Nutzung der Cookie-Daten zu informieren (§ 13 Abs. 1 TMG). Ob dies z. B. durch Pop-up-Fenster oder durch Banner auf der Startseite verbunden mit einer verlinkten näheren Erläuterung in einer Datenschutzerklärung erfolgt, bleibt dem Betreiber überlassen.

Der Nutzer kann sich allerdings auch unabhängig davon über Cookies auf seinem Rechner informieren und Maßnahmen zur vollständigen oder eingeschränkten Abwehr treffen. Alle verbreiteten Browser bieten dem Nutzer die Möglichkeit zu einer Cookie-Verwaltung. In dem in Deutschland gebräuchlichsten Browser Firefox kann sich der Nutzer sämtliche Cookies anzeigen lassen und den Inhalt der Cookies anschauen. Er kann Cookies des Servers der aufgerufenen Webseite annehmen oder ablehnen, Drittanbieter-Cookies annehmen oder ablehnen, Cookies für einzelne Webseiten oder für einzelne Sitzungen erlauben oder ablehnen und sämtliche oder einzelne Cookies löschen (s. Abb. 2).

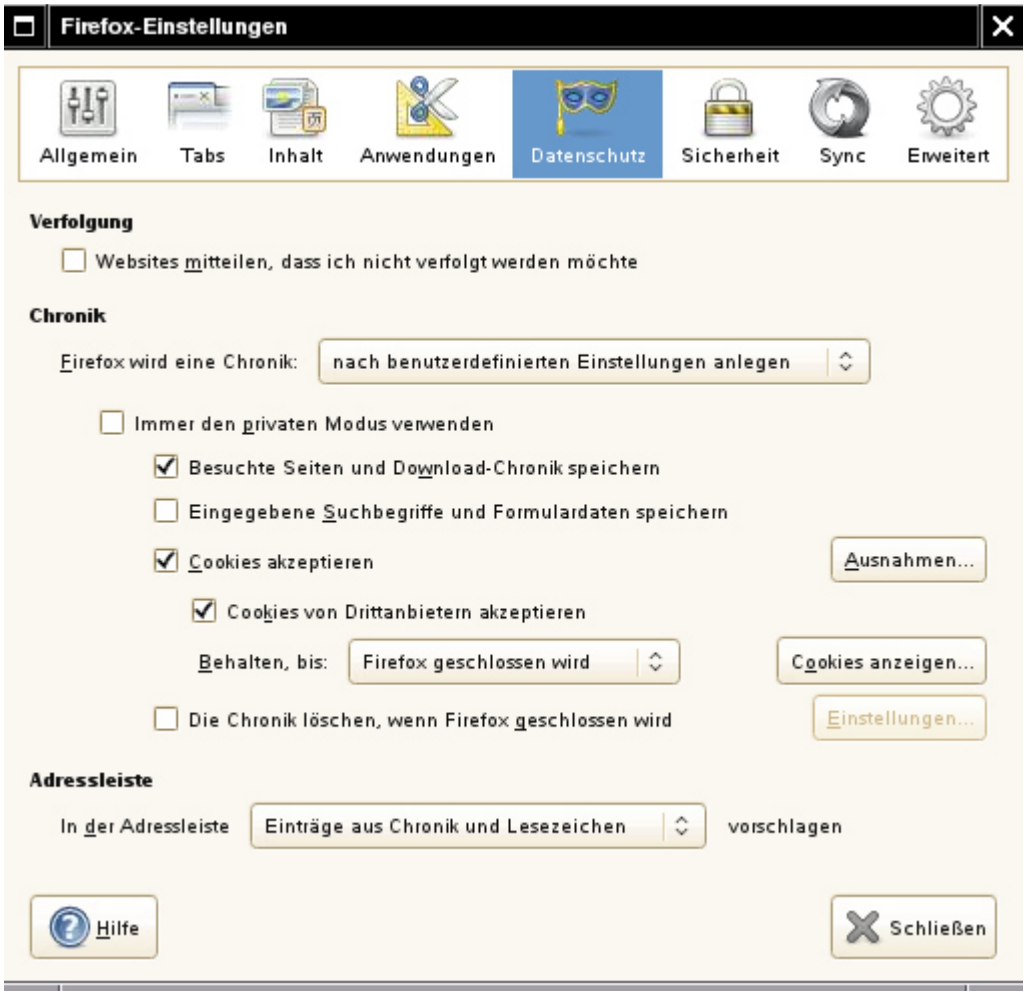

Abb. 2

Es gibt außerdem Sofwareerweiterungen (Ad-on) für Webbrowser, die Cookies anzeigen und das Blockieren ermöglichen.

6. Bilanz

6.1
„Smart Borders“ – Intelligente Außengrenzen der EU
(43. Tätigkeitsbericht, Ziff. 2.2)

Bereits im letzten Tätigkeitsbericht habe ich ausführlich über das Reformvorhaben „Smart Borders“, insbesondere vor dem Hintergrund des Urteils des EuGH zur Vorratsdatenspeicherung, berichtet. Das Gesetzespaket „Intelligente Grenzen“, das die Europäische Kommission im Jahr 2013 vorgelegt hatte, beinhaltet ein Einreise-/Ausreisesystem (EES) sowie ein Programm für registrierte Vielreisende (RTP). Im Berichtszeitraum hat sich das Vorhaben weiterentwickelt. Unter Beteiligung meiner Mitarbeiterin hat die europäische Arbeitsgruppe „Borders, Travel and Law Enforcement“ die neuen Entwicklungen intensiv diskutiert.

Mit dem geplanten „Smart Borders“-System sollen ab etwa 2020 in einer Datenbank Angaben über die Ein- und Ausreise von Drittstaatsangehörigen, das heißt von Nicht-EU-Bürgern, gespeichert werden. Im Herbst 2014 legte die Europäische Kommission die Ergebnisse einer Machbarkeitsstudie für das Reformprojekt vor, die technische Konzepte untersucht und bewertet hat. Die dort genannten Möglichkeiten für die Verarbeitung biometrischer Daten wurden ab 2015 in einer Pilotstudie an Flughäfen, Bahnhöfen und Häfen der EU getestet. Dabei kamen verschiedene Verfahren zum Einsatz, wobei zur Datenerhebung neben dem Gesichtsbild entweder vier, acht oder zehn Fingerabdrücke verwendet wurden. Zum Erfassen der Fingerabdrücke kamen die an Außengrenzen bereits vorhandenen Technologien ebenso zum Einsatz wie Scanner der „neuesten Generation“. Auch am Flughafen Frankfurt/Main wurde das Grenzkontrollsystem getestet. Die im Testverfahren erhobenen Daten wurden ausschließlich für die Testphase verwendet, um die Qualität der Daten zu beurteilen. Die Ergebnisse der Pilotstudie lagen im Berichtszeitraum noch nicht vor. Ein Zwischenbericht verwies jedoch bereits darauf, dass die automatischen Grenzkontrollsysteme möglicherweise mit Hilfe eines auf dem Ausweis aufgeklebten Chips überwunden werden können. Diese und andere technische Fragen zum „Wie“ der Umsetzung des Reformprojekts sind in den kommenden Jahren zu klären. Das „Ob“, das heißt die Frage, ob das 1,35 Mrd. EUR teure Projekt tatsächlich erforderlich ist, wurde im Berichtszeitraum nicht mehr diskutiert.

Aufgrund der hohen Kosten für das Reformpaket bestehen Bestrebungen, neben dem ursprünglichen Ziel des Vorhabens – die Aufdeckung sog. „Over-Stayer“, das heißt

Personen, die ihren Aufenthaltstitel (z. B. Visa) um die festgeschriebene Dauer überschreiten – den Anwendungsbereich des Systems „Intelligente Grenzen“ noch weiter auszudehnen. Viele Mitgliedstaaten äußerten den Wunsch, den nationalen Strafverfolgungsbehörden Zugriff auf die erhobenen Daten zu gewähren. Dieses Thema habe ich im 43. Tätigkeitsbericht (Ziff. 2.2.2) ausführlich erörtert. Ausgehend vom gegenwärtigen Stand der Diskussionen ist anzunehmen, dass diesem Wunsch Rechnung getragen wird. Die Kommission will einen überarbeiteten Textvorschlag für das Maßnahmenpaket „Smart Borders“ zu Beginn des Jahres 2016 präsentieren.

6.2
Umgang mit Patientendaten nach Schließung von Krankenhäusern (43. Tätigkeitsbericht, Ziff. 3.1.1)

In meinem vergangenen Tätigkeitsbericht habe ich über die Probleme berichtet, die im Hinblick auf die Patientendokumentation bei der Schließung eines Krankenhauses entstehen können. Sowohl bei einer geplanten Schließung als auch bei einer insolvenzbedingten Schließung eines Krankenhauses war es dazu gekommen, dass Patientenakten in nur unzureichend gesicherten Gebäuden dem Zugriff Dritter ausgesetzt waren. Die zum Teil vorherrschenden, unhaltbaren Zustände hatte ich mittels einer Bilddokumentation anschaulich gemacht. Ergänzend kam hinzu, dass die Herausgabe von Behandlungsakten an ehemalige Patienten aufgrund der Gegebenheiten erheblich erschwert bis unmöglich war.

Im Folgenden möchte ich über die aktuellen Entwicklungen informieren, die es im Anschluss an die Veranstaltung am 31.10.2014 zum Thema „Lagerung von Patientenakten bei Schließung einer Gesundheitseinrichtung“ im Hessischen Ministerium für Soziales und Integration gab. Zu diesem Gespräch war u. a. die LÄK Hessen, die Hessische Krankenhausgesellschaft, der Landesverband der Privatkliniken in Hessen, der Zentralverband Ambulanter Therapieeinrichtungen e. V. sowie der Berufsverband der in Deutschland tätigen Insolvenzverwalter eingeladen.

6.2.1
Aktueller Sachstand

Bei dem Gespräch am 31.10.2014 hatte der Verband der Insolvenzverwalter Deutschlands e. V. darauf aufmerksam gemacht, dass es für seine Mitglieder derzeit noch

an einer Orientierungshilfe fehle, wie im Falle der Insolvenz eines Krankenhauses zu verfahren ist. Die Mitglieder müssten insoweit bei entsprechenden Fällen erst selbst Erfahrungen sammeln.

Vermutlich hatte daher der Verband der Insolvenzverwalter, ebenso wie ich, große Hoffnungen in den weiteren Verlauf in dieser Sache gesetzt. Eine Rückmeldung des Hessischen Ministeriums für Soziales und Integration vom 16.06.2015 ließ mich jedoch zunächst daran zweifeln, dass hier zeitnah eine Lösung gefunden werden kann. So sah danach beispielsweise die Landesärztekammer Hessen im Hinblick auf ihre Mitglieder weder die Notwendigkeit für eine Versicherungslösung noch für eine rechtliche Regelung im Heilberufsgesetz. Angestrebt wird offenbar vielmehr weiter ein Vorgehen von Fall zu Fall.

Auch die Hessische Krankenhausgesellschaft teilte mit, dass die Gespräche mit der für sie zuständigen Versicherung zu keinem abschließenden Ergebnis geführt haben. Da die Problematik auf „Einzelfälle“ beschränkt sei, sei eine rasche Lösung nicht dringend. Eine solche Lösung werde in jedem Fall einige Zeit in Anspruch nehmen. Soweit für mich ersichtlich, machen auch die Versicherungen den Bedarf für eine solche Lösung von dem Bestehen einer gesetzlichen Regelung abhängig.

Ungeachtet dieser Entwicklungen habe ich den Dialog mit dem Hessischen Ministerium für Soziales und Integration fortgesetzt. In diesem Vorgehen wurde ich durch Presseberichte aus anderen Bundesländern bekräftigt, in denen über ähnliche Probleme mit insolventen Privatkliniken berichtet wurde. Speziell in NRW wünscht sich diesen Berichten zufolge auch das dortige Sozialministerium eine bundesgesetzliche Regelung in Bezug auf insolvente Krankenhäuser.

6.2.2
Ausblick

Wie mir mittlerweile seitens des Hessischen Ministeriums für Soziales und Integration mitgeteilt wurde, fand im November 2015 eine Sitzung der Arbeitsgemeinschaft der Obersten Landesgesundheitsbehörden (AOLG) statt.

Darin wurde mehrheitlich beschlossen, dass die Gesundheitsministerkonferenz die Bundesregierung darum bitten soll, eine Gesetzesinitiative zum BGB in die Wege zu leiten. Es ist angedacht, dass im Patientenrechtegesetz Genaueres dazu geregelt wird, wie bei der

Schließung einer Gesundheitseinrichtung mit den Patientenakten zu verfahren ist und wie das Recht der Patientinnen und Patienten auf Akteneinsichtnahme gemäß § 630g BGB gesichert wird.

Darüber hinaus konnte ich das Hessische Ministerium für Soziales und Integration dafür gewinnen, dass im Rahmen der anstehenden Änderung des Hessischen Krankenhausgesetzes auch genauer geregelt wird, wie im Falle einer geplanten Schließung eines im Krankenhausplan stehenden Krankenhauses mit den Patientenakten zu verfahren ist. Angedacht ist hier insoweit, dass verpflichtend ein Konzept für die Stilllegung vorzulegen ist, aus dem auch hervorgeht, dass und insbesondere wie der Datenverbleib sichergestellt ist.

Soweit dies die Frage zum Umgang mit Patientenakten bei der insolvenzbedingten Schließung eines nicht im Krankenhausplan stehenden Krankenhauses betrifft, ist derzeit noch keine Lösung in Sicht. Ich werde meinerseits im nächsten Jahr noch einmal eruieren, welche Lösungsmöglichkeiten es hier gibt. Gegebenenfalls kann ein solcher Ansatz über eine Regelung in der Gewerbeordnung oder in der Insolvenzordnung gefunden werden. Die entsprechende Kompetenz für eine solche Regelung liegt jedoch auch hier beim Bundesgesetzgeber.

6.3
Dauerbrenner bei Hartz IV: Vorlage und Speicherung von Kontoauszügen (34. Tätigkeitsbericht, Ziff. 5.9.1)

Seit Einführung und Umsetzung von Hartz IV kam es zu kontroversen Diskussionen anfangs auch über die Vorlage, dann verstärkt über die Speicherung von Kontoauszügen im Rahmen der Mitwirkungspflichten von Antragstellern von SGB-Leistungen. Die von mir bereits seit zehn Jahren ständig vertretene Rechtsauffassung zur zulässigen Speicherung von Kontoauszügen in Leistungsakten wurde im Berichtszeitraum durch zwei Landessozialgerichte eindeutig bestätigt.

Im Sozialrecht sind die Mitwirkungsobliegenheiten weiterhin vor allem in den §§ 60 ff. SGB I geregelt.

§ 60 Abs. 1 SGB I

Wer Sozialleistungen beantragt oder erhält, hat
1. alle Tatsachen anzugeben, die für die Leistung erheblich sind ... ,
…
3. Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen ... .
...

Kontoauszüge waren und sind unstrittig Beweisurkunden im Sinne dieser Vorschrift. Die Sozialbehörde kann deren Vorlage daher verlangen, da sie hiermit auch die finanziellen Verhältnisse aufklären kann. Diese Aufklärung der Einkommens- und Vermögensverhältnisse verlangt der Gesetzgeber in den §§ 11, 12 SGB II bei der Entscheidungsfindung über die Gewährung von Arbeitslosengeld II.

In meiner Beratungspraxis seit Einführung und Umsetzung von Hartz IV, also dem Grundsicherungsrecht nach SGB II seit 01.01.2005, habe ich es immer als datenschutzfreundlichste „Variante A“ ausdrücklich begrüßt, wenn ein schriftlicher Vermerk des Prüfergebnisses der im Rahmen der Mitwirkungspflicht vorgelegten und gesichteten Kontoauszüge von den Leistungsträgern als ausreichend erachtet und dies auch entsprechend praktiziert wurde.

Trotzdem habe ich anfragenden Petenten oder Leistungsträgern regelmäßig parallel auch immer mitgeteilt, dass ich gegen eine weniger datenschutzfreundliche „Variante B“ keine durchgreifenden datenschutzrechtlichen Bedenken habe und es daher auch nicht beanstande, wenn Kopien der vorgelegten Kontoauszüge mit zu den Akten genommen und gespeichert werden. Dies unter Berücksichtigung des datenschutzrechtlich berechtigten Anliegens von Betroffenen, dass die nicht relevanten Angaben auf den Auszügen geschwärzt werden können. Die Schwärzungsmöglichkeit besteht nach wie vor bei Ausgabebuchungen und bezieht sich jedoch nicht auf das Buchungs- und Wertstellungsdatum, sondern ausschließlich auf bestimmte Passagen des Empfängers und Buchungstextes, hier vor allem auf womöglich enthaltene besondere Arten personenbezogener Daten (Angaben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben).

Das Bayerische Landessozialgericht hat am 21.05.2014 einen Beschluss mit folgenden Leitsätzen gefasst (Az. L 7 AS 347/14 B ER):

1. Personen, die Leistungen nach dem SGB II beantragen, sind auf Aufforderung verpflichtet, dem Jobcenter Kontoauszüge für die letzten drei Monate vorzulegen.
2. Die Vorlage von Kontoauszügen zur Einsicht ist eine rechtmäßige Erhebung von Daten nach § 67a Abs. 1 Satz 1 SGB X.
3. Das Aufbewahren der Kontoauszüge in der Verwaltungsakte ist eine rechtmäßige Speicherung von Daten nach § 67c SGB X. Dabei kommt es nicht darauf an, ob die Kontoauszüge anrechenbares Einkommen ausweisen.

In seinen Entscheidungsgründen führt das Gericht zur Aufbewahrung und Speicherung der Kontoauszüge aus, diese sei erforderlich, um sie „sorgfältig auf Einkommen, Vermögen und Bedarf zu prüfen. Eine kurze Einsichtnahme genügt dafür nicht. (…) Das anrechenbare Einkommen festzustellen erfordert komplexe Berechnungen." Die am Ende des Prüfungsprozesses stehende Verwaltungsentscheidung begründe außerdem die Erforderlichkeit der Datenspeicherung mit Blick auf mögliche Widerspruchs- und Gerichtsverfahren, da sie nur so überprüfbar sei.

Auch das Landessozialgericht Berlin-Brandenburg hat in einem Beschluss vom 10.03.2015 (Az. L 31 AS 2974/14) sehr deutlich festgehalten, dass die Aufbewahrung von Kontoauszügen in Leistungsakten des Jobcenters eine rechtmäßige Datenspeicherung sei. Es ist in seinen Schlusssätzen der Entscheidungsgründe im vorliegenden Rechtsstreit sogar so weit gegangen, zu sagen, dass „der Verbleib der Kontoauszüge in den Verwaltungsakten (…) wegen ihrer Relevanz für Folgeverfahren jedenfalls in all denjenigen Fällen, in denen der Bevollmächtigte des Klägers in Erscheinung tritt, nicht nur hinzunehmen, sondern geradezu geboten" sei.

Ob das in dieser Form allgemeine Gültigkeit hat, möchte ich ebenso offen lassen wie eine Reaktion unterlassen auf den Hinweis des Gerichts in seinen Entscheidungsgründen, dass Empfehlungen der Datenschutzbeauftragten zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen „einer Überprüfung am Maßstab der Lebenswirklichkeit jedenfalls im Bereich der Grundsicherung für Arbeitsuchende nicht standhalten können".

Im Ergebnis bleibt es bei der Feststellung, dass die von mir für das Bundesland Hessen schon immer vertretene Rechtsauffassung auch durch diese beiden Urteile nochmals untermauert wird und insofern kein Anlass besteht, von dieser abzuweichen.

7. Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

7.1
Umlaufentschließung vom 05.02.2015

Keine Cookies ohne Einwilligung der Internetnutzer

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann z. B. auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie, Art. 5 Abs. 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sog. Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotenzial für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherten Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur

Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

7.2
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Datenschutz nach "Charlie Hebdo":
Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11.09.2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des

Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

7.3
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Datenschutz-Grundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

– Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

– Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang

zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

– Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

– Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

7.4
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

– eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
– die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
– die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
– kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014–2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist.[1] Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der

Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

[1]Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

7.5
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe-Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe-Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe-Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten

zugreifen und damit die Safe-Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

7.6
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BTDrucks. 18/4096 vom 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten

Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o. g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldepflicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und

leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

7.7
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine

schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

7.8
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz") würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechenden Ankündigungen ist eine Erprobung des Patientenzugriffs bislang

unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

   Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

7.9
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19.03.2015

Big Data zur Gefahrenabwehr und Strafverfolgung:

Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden (“Predictive Policing“).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf

eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

7.10
Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 09.06.2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BRDrucks. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische,

organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecke zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotenzial sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

7.11
Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 14.08.2015

Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung

I. Vorbemerkung

Nachdem der Rat der Justiz- und Innenminister am 15. Juni 2015 seinen Standpunkt zur Datenschutz-Grundverordnung abgeschlossen hat, beraten Kommission, Parlament und Rat seit Ende Juni im sogenannten Trilog über ihre verschiedenen Positionen zur Datenschutz-Grundverordnung mit dem Ziel einer Gesamteinigung und Verabschiedung des Rechtsaktes zum Jahresende 2015.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich seit der Präsentation der Vorschläge durch die Kommission im Januar 2012 mehrfach öffentlich zur Datenschutzreform positioniert. Sie hat sowohl zum gesamten Paket am 11. Juni 2012 eine Stellungnahme abgegeben als auch in einer Reihe von Entschließungen und Stellungnahmen zu einzelnen Fragen der Datenschutzreform Position bezogen.[1] Die Konferenz hat von Anfang an das Ziel der Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union bereitzustellen“[2]. Dies gilt umso mehr, als die Kommission ausdrücklich das Grundrecht des Einzelnen auf Datenschutz in den Mittelpunkt gerückt hat, dem die Reform zugutekommen soll.

Deshalb ist es für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder von außerordentlicher Bedeutung, dass die Datenschutz-Grundverordnung im Vergleich zum geltenden Rechtsstand – der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist – einen verbesserten, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Keinesfalls darf die Reform des Europäischen Datenschutzrechts dazu führen, hinter dem geltenden Datenschutzniveau zurückzubleiben. Die Konferenz betont, dass die sich aus Art. 8 der Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes daher nicht zur Disposition stehen dürfen. Nach wie vor fehlen spezifische Anforderungen an riskante Datenverarbeitungen, wie z. B. beim Profiling oder bei der Videoüberwachung. Auch sollen Daten für Werbezwecke weiterhin ohne Einwilligung der Betroffenen verarbeitet werden können. Gerade in Zeiten von Big Data und globaler Datenverarbeitung sind die Autonomie des Einzelnen, Transparenz und Rechtmäßigkeit der

---

[1] Entschließungen „Ein hohes Datenschutzniveau für ganz Europa“ vom 21./22.3.2012 sowie Stellungnahme vom 11.6.2012; „Europäische Datenschutzreform konstruktiv und zügig voranbringen!“ vom 8./9.11.2012; „Europa muss den Datenschutz stärken“ nebst Erläuterungen vom 13./14.3.2013; „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28.3.2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 18./19.3.2015, jeweils abrufbar unter http://www.bfdi.bund.de/DE/Infothek/Entschliessungen/DSBundLaender/Functions/DSK_table.html

[2] Mitteilung der Kommission, Der Schutz der Privatsphäre in einer vernetzten Welt – Ein europäischer Datenschutzrahmen für das 21. Jahrhundert, KOM(2012) 9 endg., Ziff. 6

Datenverarbeitung, die Zweckbindung oder die Verantwortlichkeit des Datenverarbeiters ebenso wichtige Elemente der Grundrechtsgewährleistung wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Bei den genannten und den im Folgenden angesprochenen Themen handelt es sich um die wichtigsten Punkte, denen sich nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die am Trilog teilnehmenden Parteien insbesondere widmen sollten.

Zur besseren Handhabbarkeit orientiert sich diese Stellungnahme an der Struktur der vorliegenden Entwürfe der Datenschutz-Grundverordnung.

II. Die Vorschläge im Einzelnen

1. Der Anwendungsbereich der Datenschutz-Grundverordnung

a) Keine Ausweitung der Haushaltsausnahme!

Der Rat hat die so genannte Haushaltsausnahme in Art. 2(2)(d) Datenschutz-Grundverordnung (DSGVO) in der Weise erweitert, dass er die im Kommissionsvorschlag enthaltenen Worte „ausschließlich“ und „ohne jede Gewinnerzielungsabsicht“ gestrichen hat.

Der Vorschlag des Rates ist in einer Weise formuliert, dass ein maßgeblicher Teil der Verarbeitung personenbezogener Daten durch natürliche Personen auch dann aus dem Anwendungsbereich des Datenschutzrechts herausfiele, wenn in erheblicher Weise in das Datenschutzgrundrecht Dritter eingegriffen würde. Nach der Formulierung des Rates würde es bereits genügen, wenn die Verarbeitung zu persönlichen oder familiären Zwecken bei einer Gesamtbetrachtung lediglich einen völlig untergeordneten Zweck darstellte, um unter die Haushaltsausnahme zu fallen und damit nicht mehr dem Datenschutzrecht zu unterliegen. Ein Nutzer eines sozialen Netzwerks oder der Betreiber einer privaten Homepage würde selbst dann nicht unter das Datenschutzrecht fallen, wenn er in großem Umfang personenbezogene Daten unbeschränkt im Internet veröffentlicht, solange er die Datenverarbeitung (auch) als eine solche zu persönlichen oder familiären Zwecken deklariert. Eine derartige Erweiterung wäre nicht akzeptabel. Ebenso wenig kann die Gewinnerzielungsabsicht ein Kriterium für die Anwendung des Datenschutzrechts sein, da die Eingriffstiefe einer Datenverarbeitung hiervon nicht abhängt. Eine zu weitgehende Ausdehnung der Haushaltsausnahme stünde im Widerspruch zum primärrechtlich

garantierten Grundrecht auf Datenschutz und kann deshalb im Sekundärrecht nicht umgesetzt werden.

Die Konferenz spricht sich gegen eine Erweiterung der Haushaltsausnahme in Art. 2(2)(d) DSGVO und die damit verbundene Einschränkung des Anwendungsbereichs des Datenschutzrechts aus. Die Haushaltsausnahme sollte sich daher weiterhin an dem Wortlaut von Art. 2(2) der Richtlinie 95/46/EG orientieren und nur solche Verarbeitungsvorgänge aus dem Anwendungsbereich herausnehmen, die sich ausschließlich auf persönliche und familiäre Tätigkeiten beziehen.

b) Keine weitere Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie!

Die DSGVO wird keine Anwendung finden, soweit die Richtlinie für den Bereich Polizei und Justiz (JI-RL) Anwendung finden wird. Somit bestimmt der Anwendungsbereich der JI-RL zugleich den Anwendungsbereich der DSGVO. Vor diesem Hintergrund hat der Rat in den letzten Monaten verschiedene Entwürfe diskutiert, die teilweise zu einer deutlichen Ausdehnung des Anwendungsbereichs der JI-RL führen könnten.

Die Konferenz sieht keine überzeugenden Gründe dafür, von der ursprünglich vorgesehenen Trennung der Anwendungsbereiche von DSGVO und der JI-RL wesentlich abzuweichen. Nach dem ursprünglichen Entwurf der KOM enthält die JI-RL Regelungen zum "Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung". Der Rat kritisiert, dass damit die präventive Gefahrenabwehr nicht erfasst ist, soweit sie der Prävention einer Straftat dient. Dies führe wiederum dazu, dass die Datenverarbeitung der Polizeien unterschiedlichen Rechtsakten unterliege. Um die gesamte Aufgabenerfüllung der Polizei unter einem Rechtsakt – der JI-RL – zusammenzufassen, soll der Anwendungsbereich der RL entsprechend erweitert werden. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltung unter die RL zu fassen.

Eine solche Ausweitung lehnt die Konferenz ab. Sofern überhaupt ein Kompromiss gefunden werden muss, der den Anwendungsbereich der JI-RL für die polizeiliche Datenverarbeitung erweitern soll, muss durch die Formulierung im Gesetzestext und in den Erwägungsgründen zumindest sichergestellt sein, dass davon nicht auch noch die Datenverarbeitung der Ordnungsverwaltung erfasst wird. Die Datenverarbeitung von anderen Behörden muss weiterhin von der DSGVO geregelt werden, wie es auch der gegenwärtige Rechtsrahmen vorsieht.

Die Konferenz spricht sich gegen die in der Ratsfassung hinzugefügte Beschränkung des Anwendungsbereichs der DSGVO zugunsten der JI-Richtlinie in Art. 2(2)(e) DSGVO aus. Die Datenverarbeitung der Ordnungsverwaltung und zur Gefahrenabwehr sollte von der DSGVO geregelt werden.

2. Für eine klare Definition des Personenbezugs!

Die DSGVO knüpft wie auch das geltende Recht weiterhin am Begriff des personenbezogenen Datums an. Dies ist die logische Konsequenz aus der grundrechtlichen und primärrechtlichen Gewährleistung in Art. 8 Abs. 1 EU-Grundrechtecharta und Art. 16 Abs. 1 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden Daten hat. Deshalb kommt der Definition des personenbezogenen Datums in Art. 4(1) DSGVO eine außerordentlich hohe Bedeutung zu, denn sie entscheidet letztlich über die Anwendbarkeit des Datenschutzrechts.

Dabei muss klargestellt sein, dass eine natürliche Person auch dann als identifizierbar anzusehen ist, wenn sie innerhalb einer Gruppe von Personen von anderen Personen unterschieden und damit auch unterschiedlich behandelt werden kann. Deshalb muss die Identifizierbarkeit einer Person auch deren Herausgreifen einschließen, wie es dem Vorschlag des Parlaments in EG 23 zugrunde liegt.

Die Vorschläge von Kommission und Rat zu EG 24 führen zudem zu einer unnötig restriktiven Auslegung des Begriffs des personenbezogenen Datums, indem sie Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten ansehen. Für diese Daten gelten die gleichen Kriterien für die Bestimmung des Personenbezugs wie für jede andere Information. Deren gesonderte Erwähnung verleitet zu dem unzulässigen Schluss, dass hier andere Kriterien gelten würden. Dies widerspräche auch der Rechtsprechung des EuGH.

Die Konferenz unterstützt insoweit den Vorschlag des Parlaments zu EG 23, wonach klargestellt ist, dass die Möglichkeit des Herausgreifens einer natürlichen Person aus einer Gruppe ein Mittel zu deren Identifizierbarkeit ist.

Die Konferenz fordert, bei EG 24 dem Vorschlag des Parlaments zu folgen, der klarstellt, dass Kennnummern, Standortdaten, Online-Kennungen, IP-Adressen oder sonstige Elemente grundsätzlich als personenbezogene Daten zu betrachten sind.

3. Datensparsamkeit muss Gestaltungsziel bleiben!

Für eine möglichst grundrechtsschonende Datenverarbeitung ist es unabdingbar, dass sich Staat und Wirtschaft auf das zur Erreichung ihrer rechtlichen oder legitimen Zwecke notwendige Maß beschränken. Die allgegenwärtige Datenverarbeitung und der Einsatz von Big-Data-Technologien erzeugen eine unvorstellbare Menge an (auch personenbezogenen) Daten. Dies führt zu einer für viele als diffus bedrohlich empfundenen Situation, da auf diese Weise Unternehmen oder Behörden potentiell in der Lage sind, über jeden Einzelnen Informationen aus sämtlichen Lebensbereichen zu erfassen und beliebig auszuwerten. Gerade deshalb ist das Prinzip von Datenvermeidung und Datensparsamkeit, das seit vielen Jahren im deutschen Datenschutzrecht verankert ist, wichtiger denn je. Auf diese Weise werden Anreize für eine datenschutzfreundliche Gestaltung von Verarbeitungs- und Geschäftsprozessen geschaffen.

Dies haben die Kommission und das Parlament erfreulicherweise auch erkannt, indem sie das Prinzip der Datensparsamkeit ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5(1)(c) DSGVO verankert haben. Umso unverständlicher ist es, dass der Rat in seinem Entwurf das Prinzip der Datenvermeidung aus dem Text gestrichen hat – ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten.

Die Konferenz spricht sich für eine ausdrückliche Verankerung des Prinzips der Datensparsamkeit in Art. 5(1)(c) DSGVO entsprechend der Formulierung der Kommission bzw. des Parlaments aus.

4. Keine Aufweichung der Zweckbindung!

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. Art. 8 Abs. 2 der Europäischen Grundrechtecharta hat daher die Zweckbindung als tragendes Prinzip des Datenschutzes verankert.

Dementsprechend folgt der Kommissionsentwurf der DSGVO grundsätzlich dem hergebrachten Ansatz der Richtlinie 95/46/EG, indem er in Art. 5(1)(b) zunächst festlegt, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige

Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen.

Die Konzeption der geltenden Richtlinie 95/46/EG ist dadurch geprägt, dass sie eine Verarbeitung personenbezogener Daten zu anderen Zwecken nur zulässt, wenn diese neuen Zwecke mit dem Ursprungszweck vereinbar sind. Weitere Zweckänderungen lässt die Richtlinie nicht zu. Auf dieser Basis ist es in der Regel gelungen, einen starken Schutz des Rechts auf informationelle Selbstbestimmung in einen angemessenen Ausgleich mit den öffentlichen Datenverarbeitungsinteressen des Staates und den legitimen Interessen der Unternehmen zu bringen.

Hiervon abweichend hat die Kommission in ihrem Vorschlag zu Art. 6(4) DSGVO zusätzlich die Möglichkeit vorgesehen, dass personenbezogene Daten auch zu solchen Zwecken weiterverarbeitet werden dürfen, die mit dem ursprünglichen Verarbeitungszweck nicht vereinbar sind. Der Rat hat diese Ausnahme noch erweitert, indem er solche Zweckänderungen auch bei einem überwiegenden berechtigten Interesse des Verarbeiters zulassen will. Spätestens durch diese Ergänzungen werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

Das Europäische Parlament ist deshalb zu dem bewährten Ansatz der Richtlinie 95/46/EG zurückgekehrt und hat konsequenterweise Art. 6(4) DSGVO gestrichen. Dies entspricht auch einer frühzeitig erhobenen Forderung der Artikel 29-Gruppe der Europäischen Datenschutzbehörden.

Die Gewährleistung einer starken Zweckbindung ist eine unabdingbare Voraussetzung, um dem Einzelnen ein Höchstmaß an Entscheidungsfreiheit und Transparenz zu ermöglichen. Die Konferenz lehnt deshalb die vom Rat vorgeschlagene Aufweichung der Zweckbindung entschieden ab und spricht sich auf der Basis des Ratsvorschlages für eine Streichung des Art. 6(4) DSGVO aus.

5. Keinen datenschutzrechtlichen Freibrief für Statistik, Archive sowie wissenschaftliche und historische Zwecke!

Die Verarbeitung personenbezogener Daten für die im öffentlichen Interesse tätigen Archive, für die Statistik sowie für historische und für Forschungszwecke folgt aufgrund der jeweiligen Eigenarten der genannten Zweckbestimmungen zum Teil besonderen Regelungen. In allen

Fällen geht es darum, die Grundrechte auf Datenschutz und Privatsphäre in einen angemessenen Ausgleich zu bringen mit wichtigen – zum Teil ebenfalls grundrechtlich – geschützten Interessen wie der Forschungsfreiheit oder den öffentlichen Interessen an der amtlichen Statistik bzw. der langzeitlichen Verfügbarmachung staatlicher Informationen durch die Archive. Dies wird grundsätzlich auch durch die Datenschutzbeauftragten des Bundes und der Länder anerkannt. Das geltende Datenschutzrecht hat diesen Ausgleich bisher angemessen hergestellt.

Der Rat geht in seinem Entwurf in verschiedener Hinsicht über diesen Ansatz hinaus und privilegiert die genannten Bereiche in unannehmbarer Weise. Einerseits soll eine Weiterverarbeitung zu den genannten Zwecken gemäß Art. 5(1)(b) DSGVO generell immer möglich sein; die Zweckbindung wird insoweit aufgehoben. Andererseits soll Art. 6(2) DSGVO die (Weiter-)Verarbeitung zu den genannten Zwecken ermöglichen, ohne dass es der Rechtsgrundlagen des Art. 6(1) DSGVO bedarf. Dies würde bedeuten, dass eine Verarbeitung zu den genannten Zwecken ohne weitere Rechtsgrundlage – vorbehaltlich mitgliedstaatlicher Sonderbestimmungen in Teilbereichen nach Art. 83 DSGVO – möglich wäre und die Weiterverarbeitung personenbezogener Daten, die ursprünglich zu anderen Zwecken erhoben worden sind, weitgehend schrankenlos möglich wäre.

Hinzu kommt, dass der gegenständliche Anwendungsbereich der Privilegierung zu weit gefasst ist. Einzig für die Archive im öffentlichen Interesse bestehen insofern keine Bedenken, zumal sich zumindest die staatlichen Archive nach Art. 83 DSGVO nach dem meist ausdifferenzierten mitgliedstaatlichen Recht zu richten haben. Bei der Privilegierung der statistischen Zwecke differenziert der Ratsentwurf hingegen nicht nach solchen der amtlichen Statistik und sonstigen statistischen Zwecken. Während für Erstere im Rahmen von Art. 83 DSGVO eine Privilegierung nachvollziehbar ist, besteht im Übrigen die Gefahr, dass etwa die Betreiber von sozialen Netzwerken, Suchmaschinen, Analysetools usw. die von ihnen vorgenommene umfassende Profilbildung als statistische Zwecke deklarieren. Vergleichbare Bedenken bestehen auch gegen die Privilegierung der wissenschaftlichen Datenverarbeitung, die vom Rat nicht auf Zwecke der wissenschaftlichen Forschung beschränkt wird, sondern darüber hinausgeht.

Datenschutzrechtliche Grundsätze gelten auch für die Verarbeitung personenbezogener Daten zu Zwecken der öffentlichen Archive, der Statistik sowie für wissenschaftliche und historische Zwecke. Die Konferenz erwartet im Trilog eine differenzierte und ausgewogene Regelung zum Schutze der genannten Interessen, die die Einschränkungen der Grundrechte auf Datenschutz und Privatsphäre auf das unabdingbar Notwendige beschränkt. Jede Verarbeitung zu den genannten Zwecken bedarf einer Rechtsgrundlage im Sinne von

Art. 6(1) DSGVO. Art. 6(2) DSGVO ist insofern missverständlich und sollte daher gestrichen werden. Darüber hinaus sollte – vergleichbar mit den Archiven – nur die amtliche Statistik privilegiert werden. Profilbildungen in sozialen Netzwerken, Suchmaschinen, durch den Einsatz von Analysetools usw. dürfen nicht privilegiert werden.

6. Die Einwilligung muss die Datenhoheit des Einzelnen sichern!

Recht auf informationelle Selbstbestimmung bedeutet seit jeher, dass der Einzelne grundsätzlich selbst über Preisgabe und Verwendung seiner personenbezogenen Daten entscheiden darf. Daraus folgt unmittelbar, dass der Einzelne grundsätzlich autonom darüber bestimmen kann, ob er eine Verarbeitung seiner personenbezogenen Daten erlaubt oder nicht. Die Einwilligung ist ein wesentliches Element, um diese Autonomie wirksam zu sichern. Sie ist deshalb in Art. 8 Abs. 2 der EU-Grundrechtecharta ausdrücklich als Legitimation für die Verarbeitung personenbezogener Daten genannt.

Kommission und Parlament haben sich im Bewusstsein dieser Bedeutung dafür entschieden, dass eine Einwilligung nur dann wirksam sein soll, wenn sie ausdrücklich erfolgt. Nur bei einer ausdrücklichen Willensbekundung kann letztlich der Nachweis erbracht werden, dass sich der Einzelne der Tragweite seiner Entscheidung bewusst wird.

Der Rat verabschiedet sich in seinem Entwurf entgegen der Grundrechtecharta von diesem Grundsatz, indem er bereits eine eindeutige Willensbekundung ausreichen lässt. Damit wird es insbesondere den global agierenden Diensteanbietern ermöglicht, durch die Verwendung pauschaler Datenschutzbestimmungen und datenschutzunfreundlicher Voreinstellungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Als datenschutzgerechte Einwilligung kann nur ein opt-in akzeptiert werden.

Es sollte zudem ein Koppelungsverbot ausdrücklich in den verfügenden Teil der DSGVO aufgenommen werden. Während Kommission und Parlament dieses in Artikel 7(4) DSGVO vorsehen, hat es der Rat gestrichen und erwähnt es lediglich in den Erwägungsgründen (EG 34).

Zur wirksamen Gewährleistung des Rechts auf informationelle Selbstbestimmung unterstützt die Konferenz den Ansatz von Kommission und Parlament, dass eine Einwilligung nur dann die Verarbeitung personenbezogener Daten legitimieren kann, wenn sie ausdrücklich abgegeben wird. In Art. 7 DSGVO sollte darüber hinaus ein Koppelungsverbot ausdrücklich geregelt werden.

7. Rechte der Betroffenen

a) Sicherstellung der Unentgeltlichkeit

Die Entwürfe der Kommission und des Parlaments sehen in Art. 12(4) DSGVO vor, dass Unterrichtungen der Betroffenen und *die auf Antrag ergriffenen Maßnahmen* zur Umsetzung der Betroffenenrechte unentgeltlich sind. Der Entwurf des Rates sieht dagegen vor, dass lediglich die Informationen gemäß Art. 14 und 14a sowie alle *Mitteilungen* gemäß den Artikeln 16 bis 19 und 32 unentgeltlich zur Verfügung gestellt werden. Damit bleibt unklar, ob auch die Umsetzung der Betroffenenrechte selbst unentgeltlich erfolgen muss oder die verantwortlichen Stellen hierfür ggf. eine Gebühr erheben können. Dafür spricht, dass nur das Auskunftsrecht (Art. 15) ausdrückliche Regelungen zur (Un-)Entgeltlichkeit enthält (vgl. Art. 15(1) und (1b)), die übrigen Betroffenenrechte hingegen nicht.

Die Unentgeltlichkeit der Ausübung und Umsetzung der Betroffenenrechte ist unabdingbare Voraussetzung für die effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung. Gebühren für die Ausübung schrecken die Betroffenen regelmäßig von der Wahrnehmung ihrer Rechte ab.

Die Konferenz spricht sich für eine unmissverständliche Regelung aus, dass die Ausübung der Betroffenenrechte und deren Umsetzung durch die verantwortlichen Stellen unentgeltlich erfolgen müssen.

b) Keine Einschränkung der Betroffenenrechte!

Die Information der Betroffenen (Art. 14, 14a DSGVO) versetzt diese in die Lage, Umfang und Risiko der Datenverarbeitung einzuschätzen. Sie ist die wesentliche Bedingung für die Schaffung von Transparenz. Der Entwurf des Rates sieht lediglich die Unterrichtung über die Identität der verantwortlichen Stelle, die Zwecke der Datenverarbeitung und die Rechtsgrundlage vor. Weitergehende Informationen sollen nur dann erforderlich sein, wenn sie unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten.

Die Konferenz lehnt Beschränkungen der Betroffenenrechte ab. Die Formulierungen des Rates führen zu Rechtsunsicherheit und lassen Raum für Interpretationen, die zu einer Absenkung des geltenden Datenschutzniveaus führen.

Die Informationspflichten der Art. 14 und 14a DSGVO beinhalten im Gegensatz zum Recht auf Auskunft (Art. 15) lediglich allgemeine, abstrakte Informationen über Art, Umfang und Zweck der Datenverarbeitung. Die Informationspflicht führt daher nicht zu exzessiven Bürokratiekosten, weil sie in standardisierter Form gegenüber den Betroffenen erfüllt werden kann. Die vom Europäischen Parlament vorgeschlagenen standardisierten Informationsmaßnahmen unter ergänzender Verwendung von Piktogrammen (Art. 13a) erachtet die Konferenz für erwägenswert.

Die Konferenz spricht sich gegen Einschränkungen der Betroffenenrechte aus und unterstützt die Position des Europäischen Parlaments.

c) Wirksame Begrenzung der Profilbildung sicherstellen!

Die Datenschutzbeauftragten des Bundes und der Länder sind der Auffassung, dass die bisherigen Vorschläge für eine Regelung von Profilbildungen in Art. 20 DSGVO nicht geeignet sind, um die Bürgerinnen und Bürger im Zeitalter von Big Data der Allgegenwart des Internets der Dinge und der in alle Lebens-, Privat- und Intimbereiche wie die Gesundheit vordringenden Technologien zur individuellen Datenerfassung und -analyse effektiv vor der Erstellung und Nutzung von Persönlichkeitsprofilen zu schützen.

Die Vorschläge von Kommission, Parlament und Rat zu Art. 20 DSGVO sind unzureichend, da keiner der Vorschläge die Profilbildung an sich besonderen Zulässigkeitsvoraussetzungen unterwirft, sondern erst das Treffen einer „automatisierten Entscheidung“ (Rat) oder einer „Maßnahme“ (KOM) auf Basis des Profilings bzw. „Profiling, das Maßnahmen zur Folge hat, die rechtliche oder ähnlich erhebliche Auswirkungen auf die Interessen der betroffenen Person hat“ (EP).

Unzulänglich ist insbesondere der Vorschlag des Rates, da er das Phänomen des Profilings in Anlehnung an Art. 15 Abs. 1 der EG-Datenschutzrichtlinie 95/46 auf das Treffen automatisierter Entscheidungen mit Rechtswirkung für den Einzelnen reduziert. Geregelt wird damit lediglich eine spezifische Folge der Datenverarbeitung im Zusammenhang mit der Auswertung von Persönlichkeitsmerkmalen, nicht aber die grundlegende Frage, zu welchen Zwecken und innerhalb welcher Grenzen Persönlichkeitsprofile überhaupt erstellt und genutzt werden dürfen. Zudem beinhaltet dieser Ansatz in der Praxis ein erhebliches Interpretations- und Umgehungspotenzial im Hinblick auf Dienste oder Anwendungen, die keine unmittelbaren Rechtswirkungen gegenüber dem Betroffenen entfalten, wie die Analyse des Nutzerverhaltens im Internet, die Analyse persönlicher Vorlieben durch ein soziales

Netzwerk, die Analyse von Bewegungsdaten oder die Analyse der Körperaktivität mittels Apps und Sensoren.

Vor diesem Hintergrund plädieren die Datenschutzbeauftragten des Bundes und der Länder für eine differenzierte Regelung der Profilbildung und -nutzung in der DSGVO, die folgende Kernelemente beinhalten sollte:

- Statt der Verkürzung auf automatisierte Einzelfallentscheidungen ist ein Ansatz zu wählen, der sämtliche Profilbildungen oder darauf basierende Maßnahmen erfasst. Diesem Ansatz entspricht am ehesten der vom Europäischen Parlament zu Artikel 20 unterbreitete Regelungsvorschlag.

- Ausnahmen vom Verbot der Profilbildung bedürfen eng begrenzter klarer Erlaubnistatbestände. Wegen ihrer hohen Sensitivität sollte zudem festgelegt werden, dass besondere Kategorien personenbezogener Daten nicht in eine Profilbildung einfließen dürfen.

- In jedem Fall sollte die Verarbeitung personenbezogener Daten zu Zwecken des Profilings stets mit einem Höchstmaß an Transparenz und Informiertheit des Betroffenen einhergehen. Der Einzelne muss wissen, wann, zu welchem Zweck und in welcher Form seine Daten im Internet oder bei der Nutzung eines Dienstes auf einem Endgerät zu Profilingzwecken verarbeitet werden, und muss hierzu seine ausdrückliche Einwilligung erteilen.

- Zudem sollte eine Verpflichtung zu frühestmöglicher Anonymisierung oder Pseudonymisierung der für die Profilbildung und -auswertung verwendeten Daten bestehen, Letzteres flankiert von einem Verbot der (Re-)Identifizierung.

In Anbetracht der wiederholt vom EuGH festgestellten Gefahren, die von Persönlichkeitsprofilen für das Grundrecht auf Datenschutz ausgehen, fordert die Konferenz, die vorliegenden Vorschläge für eine Profilingregelung im Sinne der vorgenannten Eckpunkte substanziell zu verbessern.

8. Die datenschutzrechtliche Verantwortlichkeit gilt für jede Verarbeitung personenbezogener Daten!

Die in Kapitel IV, insbesondere in Art. 22 DSGVO geregelte Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen *(Accountability)* gehört zu den zentralen Grundprinzipien eines modernen Datenschutzrechts. Die für die Verarbeitung Verantwortlichen und die Auftragsdatenverarbeiter sind in jedem Falle und ohne Einschränkungen für die Einhaltung des Datenschutzrechts verantwortlich. Dies gilt ungeachtet der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der Risiken für die Betroffenen. Ebenso müssen die für die Verarbeitung Verantwortlichen und Auftragsdatenverarbeiter uneingeschränkt in

der Lage sein, die Einhaltung ihrer Pflichten nachzuweisen. Risikobasierte Aspekte dürfen lediglich bei der Frage berücksichtigt werden, welche konkreten Maßnahmen zur Einhaltung der Pflichten zu treffen sind.

Es muss daher klargestellt werden, dass sich ein risikobasierter Ansatz nicht auf das „Ob" und die Nachweisbarkeit, sondern allenfalls auf das „Wie" der Einhaltung der Pflichten beziehen kann. Dies wird im Vorschlag der Kommission am besten verdeutlicht, in dem auf jede Relativierung verzichtet wird.

Die Konferenz spricht sich für den seitens der Kommission für Art. 22 DSGVO gewählten Ansatz aus, um zu verdeutlichen, dass die Verantwortlichkeit *(„Accountability")* ein tragendes Grundelement des Datenschutzes ist, das als solches einem risikobasierten Ansatz nicht zugänglich ist.

9. Für die Verankerung von Gewährleistungszielen beim technischen und organisatorischen Datenschutz!

Die Verarbeitung personenbezogener Daten bedarf zum Schutz der Grundrechte nicht nur eines rechtlichen, sondern auch eines technischen und organisatorischen Schutzes. Ein modernes Datenschutzrecht muss hierfür Gewährleistungsziele definieren, an denen sich die zu treffenden Maßnahmen auszurichten haben. Dies bedeutet, dass zu den klassischen Gewährleistungszielen der IT-Sicherheit spezifische Ziele hinzutreten müssen, die sich namentlich auf den Schutz personenbezogener Daten beziehen. Deshalb sind die Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, aber auch Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in der DSGVO zu verankern. Während sich Kommission und Rat in ihren Vorschlägen zu Art. 30(2) bzw. 30(1a) DSGVO im Wesentlichen auf die klassischen Ziele Verfügbarkeit, Integrität und Vertraulichkeit fokussieren, geht der Ansatz des Parlaments in Art. 30(1a) und 30(2) DSGVO i. V. m. Art. 5(1)(ea) und (eb) am weitesten.

Die Konferenz hält eine konsequente, klare und übersichtliche Verankerung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit in Art. 30 DSGVO für notwendig. Sie unterstützt insoweit die Zielrichtung des Parlaments, spricht sich allerdings für eine übersichtlichere Gestaltung aus.

10. Guter Datenschutz braucht betriebliche und behördliche Datenschutzbeauftragte!

Ungeachtet der materiellrechtlichen Bestimmungen hängt das konkrete Datenschutzniveau in Behörden und Unternehmen ganz entscheidend davon ab, welche Akzeptanz der Datenschutz vor Ort genießt und wie die Datenschutzkultur ausgeprägt ist. Hierzu können die Aufsichtsbehörden für den Datenschutz Impulse liefern und durch Kontrollen und Beratungen einen entscheidenden Beitrag leisten. Diese Aktivitäten bleiben aber notwendigerweise punktuell und sind aufgrund der unterschiedlichen Rollen nicht immer konfliktfrei. Deshalb kommt der Institution der Datenschutzbeauftragten in Unternehmen und Verwaltungen eine hohe Bedeutung zu.

Es ist deshalb erfreulich, dass sowohl Kommission als auch Parlament in Art. 35 DSGVO die verpflichtende Bestellung interner Datenschutzbeauftragter vorsehen. Allerdings sind die von beiden Institutionen gewählten Kriterien, unter denen eine Bestellung verpflichtend ist, wenig überzeugend.

Bedauerlicherweise hat sich im Rat eine europaweit geltende Verpflichtung zur Bestellung von Datenschutzbeauftragten nicht durchgesetzt. Hierbei wird vor allem mit dem bürokratischen und wirtschaftlichen Aufwand argumentiert. Nach den jahrzehntelangen Erfahrungen in Deutschland überzeugt dieses Argument nicht. Der Compliance-Aufwand für die Unternehmen ist ohne die Einbindung betrieblicher Datenschutzbeauftragter nicht unerheblich; durch deren Einsatz können zudem Sanktionen und Bußgelder oftmals vermieden werden.

Die Konferenz setzt sich nach wie vor dafür ein, dass eine verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter europaweit verbindlich vorgeschrieben wird. Während es für Behörden keine Ausnahmen geben sollte, sollten Unternehmen nicht nur ab einer bestimmten Größe oder einer bestimmten Zahl Betroffener einen Datenschutzbeauftragten bestellen, sondern in jedem Falle auch dann, wenn die Datenverarbeitung mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen verbunden ist.

11. Mehr Kontrolle über Datenübermittlungen an Behörden und Gerichte in Drittstaaten!

Seit den Enthüllungen von Edward Snowden wird intensiv über einen besseren Schutz der personenbezogenen Daten von europäischen Bürgerinnen und Bürgern gegenüber Behörden und Stellen aus Drittstaaten diskutiert. Deshalb hat das Parlament einen spezifischen Art. 43a DSGVO vorgeschlagen. Dieser stellt klar, dass Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung Verantwortlichen die Weitergabe personenbezogener Daten verlangen, in der

EU grundsätzlich weder anerkannt werden noch vollstreckbar sind, wenn dies nicht in internationalen Übereinkommen zur Amts- oder Rechtshilfe festgelegt ist. Sie stehen dann im Einzelfall unter dem Genehmigungsvorbehalt der in den Abkommen bezeichneten zuständigen Stellen.

Die Konferenz unterstützt diese Forderung ebenso wie die Artikel 29-Gruppe. Mit der Schaffung einer solchen Regelung wird die Tätigkeit ausländischer Nachrichtendienste in Europa zwar nicht unterbunden. Sie könnte jedoch in einem gewissen Umfang Transparenz über das Ausmaß der Überwachung herstellen, zur Wahrung der Verhältnismäßigkeit beitragen und vor allem Anreize zur Verabschiedung internationaler Übereinkommen schaffen.

Der Rat ist einer entsprechenden Initiative der Bundesregierung bedauerlicherweise nicht gefolgt.

Die Konferenz spricht sich weiterhin dafür aus, eine spezifische Rechtsgrundlage für die Datenübermittlung an Behörden und Gerichte in Drittstaaten zu schaffen, mit der insbesondere im Hinblick auf die nachrichtendienstliche Überwachung mehr Transparenz und Kontrolle geschaffen wird. Sie unterstützt den vom Parlament eingebrachten Vorschlag eines Art. 43a DSGVO.

Die Zuständigkeit sollte jedoch wie folgt geregelt werden: Haben ersuchender und ersuchter Staat ein Rechtshilfeabkommen oder einen ähnlichen internationalen Vertrag geschlossen, sollte die hierin bezeichnete Stelle für die Entgegennahme und Prüfung eines Ersuchens auf Datenübermittlung zuständig sein. In den Fällen, in denen eine zuständige Stelle nicht vertraglich bestimmt worden ist, kann diese Aufgabe nachrangig in die Zuständigkeit der Datenschutzaufsichtsbehörden fallen.

12. Für eine effektive und bürgernahe Zusammenarbeit der Datenschutzbehörden in Europa

Ein entscheidender Fortschritt der Datenschutz-Grundverordnung soll in einer verbesserten Zusammenarbeit der Datenschutzbehörden in Europa liegen. Um dies zu gewährleisten und auf der anderen Seite den Unternehmen einen Mehrwert zu bieten, hatte die Kommission einen sog. One-Stop-Shop, einen Kohärenzmechanismus und die Einrichtung eines Europäischen Datenschutzausschusses vorgeschlagen.

Auf Vorschlag des Rats soll es eine federführende Datenschutzbehörde geben, die einem Unternehmen am Ort seiner Hauptniederlassung als hauptsächlicher Ansprechpartner zur Verfügung steht, aber auch mit allen anderen – sei es aufgrund weiterer Niederlassungen

oder der Betroffenheit ihrer Bürger – betroffenen Aufsichtsbehörden kooperiert. Weiterhin hat der Rat Vorschläge zu einem sog. One-Stop-Shop gemacht, sodass Betroffene sich an die Aufsichtsbehörde und die Gerichte bei ihnen vor Ort wenden können. Um zu verbindlichen Entscheidungen ohne Beteiligung der Kommission zu kommen, schlägt der Rat darüber hinaus vor, den Europäischen Datenschutzausschuss mit verbindlichen Entscheidungsbefugnissen auszustatten. Hierzu ist der Ausschuss mit eigener Rechtspersönlichkeit auszustatten. Das vom Rat vorgeschlagene Modell ist für die Aufsichtsbehörden komplex, soll aber den Bürgerinnen und Bürgern eine ortsnahe Bearbeitung ihrer Anliegen und den Unternehmen einen Ansprechpartner für länderübergreifende Datenverarbeitungen verschaffen.

Die Konferenz unterstützt die Ziele des Ratsvorschlags zum sog. One-Stop-Mechanismus. Der effiziente Vollzug des Datenschutzrechts darf jedoch nicht durch die Untätigkeit der federführenden Datenschutzbehörde unterlaufen werden. Es ist eine Regelung zu schaffen, wonach die mitgliedstaatlichen Aufsichtsbehörden bei Betroffenheit ihrer Bürger von der federführenden Behörde ein aufsichtsbehördliches Einschreiten verlangen können, dessen Ablehnung zu einer unmittelbaren Überprüfung durch den Europäischen Datenschutzausschuss führt.

Der One-Stop-Shop soll einen ausgewogenen Ausgleich zwischen den verschiedenen Interessen schaffen, eine bürgernahe Bearbeitung von Beschwerden ermöglichen, den Unternehmen klare Ansprechpartner zur Verfügung stellen und durch die Aufwertung des Europäischen Datenschutzausschusses die notwendige Verbindlichkeit und damit Rechtssicherheit aufweisen. Die Konferenz bittet die am Trilog beteiligten Parteien gleichwohl, praktikable Verfahrensregeln festzulegen. Dies betrifft insbesondere die Frage der Verfahrensfristen und der Amtshilfe der Aufsichtsbehörden untereinander.

13. Für einen starken Beschäftigtendatenschutz

Die DSGVO überlässt die Regelung des Datenschutzes für Beschäftigte in Artikel 82 dem mitgliedstaatlichen Recht. Der Rat und die Kommission legen fest, dass die Mitgliedstaaten dabei den Rahmen der DSGVO einhalten müssen, und verzichten auf konkretere Anforderungen. Das Europäische Parlament gibt dagegen ganz konkrete Mindeststandards im Verordnungstext vor.

Die Konferenz hält es für wichtig, dass Artikel 82 DSGVO den Mitgliedstaaten in jedem Falle die Möglichkeit eröffnet, auch über den Standard der DSGVO hinausgehen zu können. Die Konferenz begrüßt den Ansatz des Parlaments, konkrete Mindeststandards für den Beschäftigtendatenschutz im Verordnungstext selbst vorzusehen.

Im Kontext der Verarbeitung von Beschäftigtendaten sollte es die Datenschutz-Grundverordnung den Mitgliedstaaten ermöglichen, im Sinne einer Mindestharmonisierung auch über das Datenschutzniveau der Verordnung hinauszugehen. Die Konferenz unterstützt den Ansatz des Parlaments, konkrete Mindeststandards festzulegen.

14. Recht auf pseudonyme Internet-Nutzung für alle Menschen in Europa schaffen!

Es gibt zahlreiche gewichtige Gründe, bei der Nutzung von Telemediendiensten auf ein Pseudonym zurückzugreifen: Dazu gehört etwa der Wunsch, einer Profilbildung unter dem realen Namen zu entgehen, sei es um sich vor rechtswidrigen Zugriffen zu schützen, sei es zur Stärkung des Schutzes bei der Nutzung sozialer Netzwerke. Ein Pseudonym kann ferner vor politischer oder rassistischer Verfolgung oder Diskriminierung und sozialer Benachteiligungen etwa wegen der sexuellen Ausrichtung schützen. Pseudonyme können schließlich verhindern, dass die private Nutzung eines Telemediums zur geschäftlichen Kontaktaufnahme durch Dritte missbraucht wird. Das ist gerade bei Berufsgeheimnisträgern wie Ärzten, Seelsorgern, Anwälten oder Sozialarbeitern nicht zuletzt zum Schutz der mit ihnen in Kontakt stehenden Personen von Bedeutung.

Das Recht, in Telemedien grundsätzlich auch unter einem Pseudonym gegenüber anderen Nutzern aufzutreten, stärkt sowohl die informationelle Selbstbestimmung Betroffener als auch die Meinungsfreiheit, ohne eine Verfolgung und Ahndung von missbräuchlichem Verhalten von unter Pseudonym auftretenden Nutzern durch den Telemedienanbieter auszuschließen. In der Europäischen Datenschutz-Grundverordnung fehlt jedoch im Katalog der Rechte Betroffener eine entsprechende ausdrückliche Regelung.

Die Konferenz hält es für erforderlich, zum Schutz der Privatsphäre der Telemediennutzer eine Bestimmung aufzunehmen, die zumindest bei zu privaten Zwecken genutzten Telemedien innerhalb der EU ein Recht auf pseudonyme Nutzung verbindlich statuiert.

7.12

Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 30.09./01.10.2015

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystemhersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezogenen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der

Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten, vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als datenverarbeitende Stelle gerecht werden können.

7.13
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 30.09./01.10.2015

Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem "Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes" (BRDrucks. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 "Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende

gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 "Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben"). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 "Effektive Kontrolle von Nachrichtendiensten herstellen!").

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

8. Beschlüsse des Düsseldorfer Kreises

8.1
Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 15./16.09.2015

Nutzung von Kameradrohnen durch Private

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potenziell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne

des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KunstUrhG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KunstUrhG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche [§ 201a des Strafgesetzbuches (StGB)], mithin Bereiche der Intimsphäre (im Einzelnen dazu: BTDrucks. 15/2466, S. 5.) oder der Aufzeichnung des nicht-öffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

8.2
Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 19.02.2014 (Stand 10.08.2015)

Videoüberwachung in Schwimmbädern – Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen. Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vgl. OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken, ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen.[1]

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens. Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z. B. Beschädigung von Haartrocknern).

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z. B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

[1]OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch – wenn auch nicht ununterbrochen – auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

9. Materialien

9.1
Positionspapier der unabhängigen Datenschutzbehörden des Bundes und der Länder zu Safe Harbor vom 21.10.2015

1. Nach dem Safe-Harbor-Urteil des EuGH vom 06.10.2015 ist eine Datenübermittlung aufgrund der Safe-Harbor-Entscheidung der Kommission vom 26.07.2000 (2000/520/EG) nicht zulässig.

2. Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt.

3. Der EuGH stellt fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten ungeachtet von Kommissions-Entscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemessenheit des Datenschutzniveaus in Drittstaaten zu beurteilen.

4. Der EuGH fordert die Kommission und die Datenschutzbehörden auf, das Datenschutzniveau in den USA und anderen Drittstaaten (Rechtslage und Rechtspraxis) zu untersuchen, und gibt hierfür einen konkreten Prüfmaßstab mit strengen inhaltlichen Anforderungen vor.

5. Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe Harbor gestützte Datenübermittlungen in die USA erlangen, werden sie diese untersagen.

6. Die Datenschutzbehörden werden bei Ausübung ihrer Prüfbefugnisse nach Art. 4 der jeweiligen Kommissionsentscheidungen zu den Standardvertragsklauseln vom 27.12.2004 (2004/915/EG) und vom 05.02.2010 (2010/87/EU) die vom EuGH formulierten Grundsätze, insbesondere die Randnummern 94 und 95 des Urteils, zugrunde legen.

7. Die Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen erteilen.

8. Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten. Unternehmen, die Daten in die USA oder andere Drittländer exportieren wollen, sollten sich dabei auch an der Entschließung der DSK vom 27.03.2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und an der Orientierungshilfe „Cloud Computing“ vom 09.10.2014 orientieren.

9. Eine Einwilligung zum Transfer personenbezogener Daten kann unter engen Bedingungen eine tragfähige Grundlage sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.

10. Beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein.

11. Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.

12. Die Kommission wird aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit. Ferner gilt es, zeitnah die Entscheidungen zu den Standardvertragsklauseln an die in dem EuGH-Urteil gemachten Vorgaben anzupassen.

    Insoweit begrüßt die DSK die von der Art. 29-Gruppe gesetzte Frist bis zum 31.01.2016.

13. Die DSK fordert die Bundesregierung auf, in direkten Verhandlungen mit der US-Regierung ebenfalls auf die Einhaltung eines angemessenen Grundrechtsstandards hinsichtlich Privatsphäre und Datenschutz zu drängen.

14. Die DSK fordert Kommission, Rat und Parlament auf, in den laufenden Trilog-Verhandlungen die strengen Kriterien des EuGH-Urteils in Kapitel V der Datenschutz-Grundverordnung umfassend zur Geltung zu bringen.

9.2

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)

Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge

Vorbemerkung

Bereits heute benötigt und produziert das moderne Kraftfahrzeug eine Vielzahl an Daten. Aufgrund der fortschreitenden informationstechnischen Ausstattung der Kraftfahrzeuge und deren Anbindung an das Internet sowie der Vernetzung der Verkehrsteilnehmer untereinander wird sich dieser Trend fortsetzen und in den kommenden Jahren zu weitreichenden Veränderungen im Straßenverkehr führen. Darüber hinaus entstehen zahlreiche neue Fahrzeugfunktionen und Verkehrstelematikanwendungen, z. B. in den Bereichen Service und Multimedia. Die Digitalisierung und insbesondere die Vernetzung bergen neben den unbestreitbaren Vorteilen für die Verkehrssicherheit und den Komfort zugleich auch Risiken für die Persönlichkeitsrechte der Fahrzeugnutzer. Vor diesem Hintergrund halten die unabhängigen Datenschutzbeauftragten des Bundes und der Länder und der VDA nachfolgende datenschutzrechtliche Aspekte für besonders relevant.[1]

1. **Personenbezogenheit:** Bei der Nutzung eines modernen Kraftfahrzeugs wird permanent eine Vielzahl von Informationen erzeugt und verarbeitet. Insbesondere bei Hinzuziehung weiterer Informationen können die anfallenden Daten auf den Halter oder auch auf den Fahrer und Mitfahrer zurückführbar sein und Informationen über persönliche oder sachliche Verhältnisse einer bestimmbaren Person enthalten. Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt.

2. Entscheidend ist der **Zeitpunkt der Datenerhebung** durch eine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes. Hier ist zu unterscheiden, ob es sich um Kraftfahrzeuge handelt, bei denen eine Datenspeicherung innerhalb des Fahrzeuges stattfindet („offline“), oder ob eine Übermittlung von Daten aus dem Fahrzeug heraus erfolgt

(„online“), wie etwa bei der Übermittlung und Speicherung von Fahrzeugdaten auf Backend-Servern. Bei „Offline“-Autos ist von einer Datenspeicherung ohne vorherige Erhebung auszugehen. Eine Erhebung liegt mangels Erfüllung des Tatbestandes des § 3 Abs. 3 BDSG nicht vor; gleichwohl fallen anlässlich der Kfz-Nutzung Daten an, die im Fahrzeug abgelegt werden. Diese Daten müssen geschützt werden und machen – vergleichbar der Regelung in § 6c BDSG (Mobile personenbezogene Speicher- und Verarbeitungsmedien) – auch eine Sicherung des Rechts auf informationelle Selbstbestimmung erforderlich. Erst wenn die im Fahrzeug abgelegten Daten z. B. von einer Werkstatt für Reparaturzwecke ausgelesen werden, kommt es zu einer Erhebung durch eine verantwortliche Stelle nach § 3 Abs. 3 BDSG.

Bei „Online“-Autos findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch eine verantwortliche Stelle im Sinne des § 3 Abs. 3 BDSG statt.

3. **Verantwortliche Stelle:** Auch für die Identifikation der verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG ist zwischen „Offline“- und „Online“-Autos zu differenzieren.

Bei „Offline“-Autos wird derjenige, der personenbezogene Fahrzeugdaten aus dem Fahrzeug ausliest (d. h. erhebt) und anschließend verarbeitet, zur verantwortlichen Stelle. Hierbei wird es sich in der Regel um Werkstätten handeln.

Auch wenn die Hersteller bei „Offline“-Autos regelmäßig mangels Erhebung nicht bereits beim „Entstehen“ der Daten verantwortliche Stelle sind, trifft diese unter anderem nach dem Gedanken „Privacy by Design“ dennoch eine Verantwortung im Hinblick auf den Datenschutz. Dies gilt insbesondere, weil der Hersteller im Rahmen seiner technischen Gestaltungsmöglichkeiten (Art und Umfang von Schnittstellen, Zugriffsmöglichkeiten, Verfolgung der in § 3a BDSG niedergelegten Grundsätze von Datenvermeidung und -sparsamkeit) Einfluss auf die zeitlich nach hinten verlagerte Erhebung und Verarbeitung hat (vergleichbar der Regelung in § 6c BDSG). Sofern es um die technischen Gestaltungsmöglichkeiten geht, sind die Hersteller auch bei dieser Fahrzeugkategorie als Ansprechpartner für die Datenschutzaufsichtsbehörden anzusehen.

Bei „Online“-Autos sind diejenigen als verantwortliche Stellen anzusehen, die personenbezogene Daten erhalten, d. h. in der Regel die Hersteller und gegebenenfalls dritte Dienste-Anbieter. Insbesondere wenn Hersteller Zusatzdienstleistungen für das Kfz

anbieten und dabei in ihren Backend-Servern Daten speichern, sind sie verantwortliche Stelle für diese Datenverarbeitung.

4. Die **Zulässigkeit der Datenerhebung und -verarbeitung** kann sich insbesondere aus § 28 Abs. 1 S. 1 Nrn. 1 oder 2 BDSG, §§ 11 ff. Telemediengesetz oder aus einer Einwilligung ergeben, die den Voraussetzungen des § 4a BDSG genügt.

Wie die Informationen über Datenerhebungs- und -verarbeitungsvorgänge aufbereitet sein müssen, um Teil des Vertrags oder Grundlage für eine ggf. relevante informierte Einwilligung sein zu können (ausführliche Informationen im Sinne eines Verfahrensverzeichnisses oder strukturierte, überblicksartige Informationen), bleibt Frage des Einzelfalls. Der Erstkäufer kann die notwendigen Informationen jedenfalls vom Verkäufer (Hersteller oder herstellergebundener Händler) erhalten.

Grundsätzlich sind die wichtigsten Informationen zur Datenverarbeitung in allgemein verständlicher Form auch in der Borddokumentation nachlesbar vorzuhalten, die der Hersteller bereitstellt.

5. Gegenüber dem Hersteller besteht ein unentgeltliches **Auskunftsrecht** des Halters über seine durch den Hersteller erhobenen und gespeicherten personenbezogenen Daten nach § 34 BDSG. Darüber hinaus besteht aus § 34 BDSG kein datenschutzrechtliches Auskunftsrecht des Halters gegenüber dem Hersteller allein aufgrund dessen Gesamtverantwortung für die Gestaltung der datenspeichernden Systeme. Die Fahrzeughalter von „Offline“-Autos haben die Möglichkeit des Auslesens von Daten, ggf. mithilfe von Sachverständigen, was nicht zwingend unentgeltlich sein muss. Aufgrund des Transparenzgebots muss der Betroffene sich unentgeltlich und ohne sachverständige Hilfe über die Grundsätze der Datenverarbeitungsvorgänge einschließlich zumindest der Art der verarbeiteten personenbezogenen Daten beim Hersteller informieren können.

6. In Bezug auf die **Datenhoheit** sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können. Die Automobilhersteller streben an, durch standardisierte Symbole im Cockpit den aktuellen Vernetzungsstatus des Fahrzeugs erkennbar anzuzeigen und Möglichkeiten der jederzeitigen Aktivierung und Deaktivierung dieses Status vorzusehen. Einschränkungen der

Löschbarkeit bestehen bei rechtlichen Verpflichtungen oder dann, wenn entsprechende Daten im Zusammenhang mit Garantie- sowie Gewährleistungen oder der Produkthaftung von Bedeutung sind oder deren Verfügbarkeit für den sicheren Fahrzeugbetrieb erforderlich ist. Vom Nutzer eingegebene Informationen (z. B. Komfortdaten wie Sitzeinstellung, bevorzugte Radiosender, Navigationsdaten, E-Mail-/SMS-Kontaktdaten etc.) muss der Nutzer jederzeit selbst ändern oder zurückstellen können.

[1] Datenschutzrechtliche Fragestellungen, die sich bei der Besitzüberlassung eines Kfz z. B. im Rahmen eines Dienst- oder Arbeitsverhältnisses oder einer Vermietung ergeben, sind nicht Gegenstand des vorliegenden Papiers.

Sachwortverzeichnis zum 44. Tätihkeitsbericht