Siebenundvierzigster Tätigkeitsbericht zum Datenschutz
und
Erster Bericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2018 gemäß
§ 30 des Hessischen Datenschutzgesetzes (bis 24. Mai 2018) und
Art. 59 der Verordnung (EU) Nr. 2016/679 (ab 25. Mai 2018) i. V. m. § 15
des Hessischen Datenschutz- und Informationsfreiheitsgesetzes sowie
§ 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Beiträge zum Datenschutz und zur Informationsfreiheit
Herausgegeben vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit
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

Gestaltung: Satzbüro Peters, www.satzbuero-peters.de
Herstellung: AC medienhaus GmbH, Ostring 13, 65205 Wiesbaden-Nordenstadt

Inhaltsverzeichnis

Verzeichnis der Abkürzungen

a. a. O.	am angegebenen Ort
a. F.	alte Fassung
Abb.	Abbildung
Abs.	Absatz
AG	Aktiengesellschaft
AK Technik	Arbeitskreis Technik
Art.	Artikel
ATDG	Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz)
BDSG	Bundesdatenschutzgesetz
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz)
BRDrucks.	Bundesratsdrucksache
BTDrucks.	Bundestagsdrucksache
BVerfSchG	Bundesverfassungsschutzgesetz
bzw.	beziehungsweise
ca.	cirka
ccTLD	country code Top Level Domain
CNIL	Commission Nationale de l'Informatique et des Libertés
d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsche Industrie-Norm(en)
DNS	Domain Name System
DSFA	Datenschutzfolgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

e. V.	eingetragener Verein
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA	Europäischer Datenschutzausschuss
EN	European Norm
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
grds.	grundsätzlich
GVG	Gerichtsverfassungsgesetz
HDBI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HMDIS	Hessisches Ministerium des Innern und für Sport
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HVSG	Hessisches Verfassungsschutzgesetz
i. d. R.	in der Regel
i. S. d.	im Sinne der/des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
insb.	insbesondere
InsO	Insolvenzordnung
ISO	International Organization for Standardization (Internationale Normierungsorganisation)
IT	Informationstechnik
KIS	Krankenhausinformationssystem
KMU	kleine und mittlere Unternehmen

LfV	Landesamt für Verfassungsschutz
lit.	littera
LKA	Landeskriminalamt
LKG Berlin	Landeskrankenhausgesetz Berlin
LKHG M-V	Krankenhausgesetz für das Land Mecklenburg-Vorpommern
LTDrucks.	Landtagsdrucksache
m. E.	meines Erachtens
o. g.	oben genannt/genannte/genannter/genanntes
OH KIS	Orientierungshilfe Krankenhausinformationssysteme
OWiG	Gesetz über Ordnungswidrigkeiten
PKK	Parlamentarische Kontrollkommission
Quellen-TKÜ	Online-Telekommunikationsüberwachung
Rdnr.	Randnummer
RED-G	Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz)
S.	Seite oder Satz
s.	siehe
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
sog.	sogenannte/sogenannter/sogenanntes
StAnz.	Staatsanzeiger für das Land Hessen
StPO	Strafprozessordnung
TOM	Technisch organisatorische Maßnahme
u. a.	unter anderem
u. U.	unter Umständen
UAG DSFA	Unterarbeitsgruppe Datenschutzfolgenabschätzung
US(A)	Vereinigte Staaten von Amerika
usw.	und so weiter
vgl.	vergleiche

VIP	very important person (sehr wichtige Person)
VISZG	Gesetz über den Zugang von Polizei- und Strafverfolgungsbehörden sowie Nachrichtendiensten zum Visa-Informationssystem (VIS-Zugangsgesetz)
VPN	Virtual Private Network
WP	Working Paper
z. B.	zum Beispiel
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften*

*Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union vom 26.10.2012 (ABl. EU C 326/47)
ATDG	Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) i. d. F. vom 22.12.2006 (BGBl. I S. 3409), zuletzt geändert durch Gesetz vom 14.08.2017 (BGBl. I S. 3202)
BDSG-alt	Bundesdatenschutzgesetz i. d. F. vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618) m. W. v. 09.11.2017, außer Kraft getreten am 25.05.2018 aufgrund Gesetzes vom 30.06.2017 (BGBl. I S. 2097)
BDSG-neu	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42, berichtigt S. 2909, 2003 S. 738), geändert durch Gesetz vom 18.12.2018 (BGBl. I S. 2639)
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz) i. d. F. vom 01.06.2017 (BGBl. I S. 1345)
BO	Berufsordnung für die Ärztinnen und Ärzte in Hessen vom 02.09.1998 (HÄBL 10/1998 S. I–VIII),), zuletzt geändert am 27.11.2018 (HÄBL 2/2019 S. 137)
BRAO	Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618)
BVerfGG	Gesetz über das Bundesverfassungsgericht i. d. F. vom 11.08.1993 (BGBl. I S. 1473), zuletzt geändert durch Gesetz vom 08.10.2017 (BGBl. I S. 3546)
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz) i. d. F. vom 20.12.1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Gesetz vom 30.06.2017 (BGBl. I S. 2097)

GRCh	Charta der Grundrechte der Europäischen Union vom 26.10.2012 (ABl. EU C 326 S. 391)
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU L 119 S. 1)
EGovG	Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) i. d. F. vom 25.07.2013 (BGBl. I S. 2749), zuletzt geändert durch Gesetz vom 05.07.2017 (BGBl. I S. 2206)
GVG	Gerichtsverfassungsgesetz i. d. F. vom 09.05.1975 (BGBl. I S. 1077), zuletzt geändert durch Gesetz vom 12.07.2018 (BGBl. I S. 1151)
GWB	Gesetz gegen Wettbewerbsbeschränkungen i. d. F. vom 26.06.2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Gesetz vom 12.07.2018 (BGBl. I S. 1151)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 07.01.1999 (GVBl. I S. 98), außer Kraft gesetzt am 25.05.2018 durch Gesetz vom 03.05.2018 (GVBl. S. 82)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018
HEGovG	Hessisches Gesetz zur Förderung der elektronischen Verwaltung (Hessisches E-Government-Gesetz) i. d. F. vom 12.09.2018 (GVBl. S. 570)
Heilberufsgesetz	Gesetz über die Berufsvertretungen, die Berufsausübung, die Weiterbildung und die Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Tierärzte, Apotheker, Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten i. d. F. vom 07.02.2003 (GVBl. I S. 66, 242), zuletzt geändert durch Gesetz vom 03.05.2018 (GVBl. S. 82)
HKHG 2011	Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2011) i. d. F. vom 21.12.2010 (GVBl. I S. 587), zuletzt geändert durch Gesetz vom 13.09.2018 (GVBl. S. 599)
HSchG	Hessisches Schulgesetz i. d. F. vom 30.06.2017 (GVBl. S. 150), zuletzt geändert durch Gesetz vom 03.05.2018 (GVBl. S. 82).
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14.01.2005 (GVBl. I S. 14, geändert durch Gesetz vom 23.08.2018 (GVBl. S. 374)

HVSG	Hessisches Verfassungsschutzgesetz i. d. F. vom 25.06.2018 (GVBl. S. 302)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz i. d. F. vom 15.01.2010 (GVBl. I S. 18), zuletzt geändert durch Gesetz vom 12.09.2018 (GVBl. S. 570)
IHKG	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern in der im BGBl. Teil III, Gliederungsnummer 701-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 29.03.2017 (BGBl. I S. 626)
InsO	Insolvenzordnung vom 05.10.1994 (BGBl. I S. 2866), zuletzt geändert durch Gesetz vom 23.06.2017 (BGBl. I S. 1693)
JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119 S. 89)
KunstUrhG (KUG)	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 16.02.2001 (BGBl. I S. 266, 280)
LKG Berlin	Landeskrankenhausgesetz vom 18.09.2011 (GVBl. S. 483), zuletzt geändert durch Gesetz vom 02.02.2018 (GVBl. S. 160)
LKHG M-V	Krankenhausgesetz für das Land Mecklenburg-Vorpommern vom 20.05.2011 (GVOBl. M-V 2011, S. 327), zuletzt geändert durch Gesetz vom 16.05.2018 (GVOBl. M-V S. 183, 185)
OWiG	Gesetz über die Ordnungswidrigkeiten i. d. F. vom 19.02.1987 (BGBl. I S. 602); zuletzt geändert durch Gesetz vom 17.12.2018 (BGBl. I S. 2571)
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz) i. d. F. vom 14.08.2017 (BGBl. I S. 3122, 3138), in Kraft getreten am 18.08.2017

RED-G	Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz) i. d. F. vom 20.08.2012 (BGBl. I S. 1798), zuletzt geändert durch Gesetz vom 14.08.2017 (BGBl. I S. 3202)
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil – i. d. F. vom 11.12.1975 (BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 17.08.2017 (BGBl. I S. 3214)
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz – i. d. F. vom 18.01.2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 18.12.2018 (GVBl. I S. 2639
StGB	Strafgesetzbuch i. d. F. vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 18.12.2018 (BGBl. I S. 2639)
StPO	Strafprozeßordnung i. d. F. vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 18.12.2018 (BGBl. I S. 2639)
TPG	Gesetz über die Spende, Entnahme und Übertragung von Organen und Geweben (Transplantationsgesetz) i. d. F. vom 04.09.2007 (BGBl. I S. 2206), zuletzt geändert durch Gesetz vom 18.07.2017 (BGBl. I S. 2757)
VISZG	Gesetz über den Zugang von Polizei- und Strafverfolgungsbehörden sowie Nachrichtendiensten zum Visa-Informationssystem (VIS-Zugangsgesetz) i. d. F. vom 06.05.2009, zuletzt geändert durch Gesetz vom 26.07.2016 (BGBl. I S. 1818)

Kernpunkte

1. Im Vordergrund des vorliegenden Tätigkeitsberichts stehen die Datenschutzreform und die Schaffung eines Informationsfreiheitsrechts. Er gliedert sich daher erstmals in einen Datenschutzbericht (geteilt für die Zeit vor bzw. nach Geltung der Datenschutz-Grundverordnung) und einen Bericht nach dem Informationsfreiheitsgesetz.
2. Das Datenschutzrecht entwickelte sich im Berichtsjahr in der EU, den Mitgliedstaaten und Deutschland unterschiedlich (Erster Teil, Ziff. 2.1 bis 2.3). In Hessen wurden mit einem Artikelgesetz das Hessische Datenschutz- und Informationsfreiheitsgesetz geschaffen und zahlreiche Änderungen in Fachgesetzen vorgenommen (Erster Teil, Ziff. 2.4).
3. Das Hessische Verfassungsschutzgesetz und das Hessische Gesetz über die öffentliche Sicherheit und Ordnung wurden zum Teil umfassend novelliert (Erster Teil, Ziff. 2.5 und Ziff. 2.6). Durch EU-Verordnungen, Bundesgesetze und Landesgesetz sind zusätzliche Prüfpflichten für den HBDI entstanden (Erster Teil, Ziff. 2.7). Ein Gesetzentwurf, mit dem im Hessischen Krankenhausgesetz eine Regelung für die Schließung eines Krankenhauses eingefügt werden soll, wurde mir vorgestellt (Erster Teil, Ziff. 5.3).
4. Mit der datenschutzrechtlich begleiteten Einführung der App „BAföGdirect“ und den Vorarbeiten zu interoperablen Servicekonten zur Bereitstellung online angebotener Verwaltungsleistungen wurden weitere Bausteine zur Strategie „Digitales Hessen 2020“ umgesetzt (Erster Teil, Ziff. 3.5.2 und Ziff. 3.5.3). Auch die Umsetzung des Projekts „Digitale Modellbehörde“ mit dem Teilprojekt „Anerkennungsprämie“ ist datenschutzrechtlich auf einem guten Weg (Erster Teil, Ziff. 4.3.1 und Ziff. 4.3.2).
5. Das Projekt „Schule ohne Rassismus – Schule mit Courage“ muss datenschutzrechtlich nachgebessert werden (Erster Teil, Ziff. 4.4.3). Das Digitalisierungsprojekt „Schultagebuch für Kinder beruflich Reisender“ (Digitales Lernen unterwegs – DigLu) schreitet voran (Erster Teil, Ziff. 5.1). Die hessenweite Einführung der Lernverlaufsdiagnostik-Software „quop“ habe ich datenschutzrechtlich begleitet und im Hinblick auf die neuen Anforderungen der DS-GVO beraten (Erster Teil, Ziff. 4.4.2).
6. Seit Geltung der Datenschutz-Grundverordnung dominieren die Eingaben im öffentlichen und nicht-öffentlichen Bereich zu den Rechten der Betroffenen. Exemplarisch werden für beide Bereiche typische Beschwerden und Fragestellungen zum Auskunftsanspruch (Erster Teil, Ziff. 4.3.4, Ziff. 4.5.2 und Ziff. 4.7.2), zur Meldung von internen Datenschutzbeauftragten, zur Information der Betroffenen (Erster Teil, Ziff. 4.6.1), zur Aufzeichnung von

Telefongesprächen, zu Bild- und Videoaufnahmen (Erster Teil, Ziff. 4.1 und Ziff. 4.3.6) sowie zur Veröffentlichung von Beschäftigtenfotos (Erster Teil, Ziff. 4.9.1) behandelt.

7. Mit der Änderung des Geschäftsmodells von Microsoft, für die Microsoft Cloud Deutschland mit dem Treuhändermodell keine Neukundenverträge mehr zu schließen, wird der Einsatz des Produkts Microsoft 365 bzw. Azure an Schulen in Frage gestellt (Erster Teil, Ziff. 5.2).
8. Die Europäisierung des Bußgeldverfahrens führt zu einer Kollision mit nationalem Verfahrensrecht (Erster Teil, Ziff. 4.11.1). Erste Erfahrungen mit den Bußgeldverfahren nach DS-GVO wurden gemacht (Erster Teil, Ziff. 4.11.2). Erste Erfahrungsberichte zu Meldungen von Datenpannen werden dargestellt (Erster Teil, Ziff. 4.11.3 und Ziff. 4.11.4).
9. Im Gesundheitsbereich war der Umgang mit Patientenakten immer wieder Thema. Die Weigerung von Patienten und Patientinnen, den Informationsflyer nach Art. 13 DS-GVO zu unterzeichnen, führte zur unzulässigen Ablehnung der ärztlichen Behandlung (Erster Teil, Ziff. 4.6.2).
10. Die datenschutzrechtliche Absicherung beim Datentransfer in die Vereinigten Staaten, das Privacy Shield, stand erneut auf dem Prüfstand (Erster Teil, Ziff. 4.2.1). Für die europaweite Zusammenarbeit des HBDI mit anderen europäischen Aufsichtsbehörden nach DS-GVO wurden erste Strukturen geschaffen (Erster Teil, Ziff. 4.2.2).
11. Interessante Entwicklungen sind in dem Bereich rund um das Kraftfahrzeug zu verfolgen. Die datenschutzrechtliche Zulässigkeit von Unfalldatenspeichern ist nur mit entsprechenden Informationspflichten zu fassen (Erster Teil, Ziff. 4.5.1). Eine breit angelegte Prüfaktion von Autowerkstätten zeigte Datenschutzmängel im Umgang mit den Fahrzeugdaten auf (Erster Teil, Ziff. 4.5.3).
12. Im ersten Tätigkeitsbericht zum Informationsfreiheitsgesetz stelle ich die verfassungsrechtlichen Grundsätze sowie erste Erfahrungen aus der Praxis dar (Zweiter Teil, Ziff. 1 bis 3).

Erster Teil
47. Tätigkeitsbericht zum Datenschutz

1. Einführung

1.1
Umbruchsituation

Der vorliegende 47. Tätigkeitsbericht ist der letzte Tätigkeitsbericht der 19. Wahlperiode des Hessischen Landtags vom 18.01.2014 bis 17.01.2019. In diesem Zeitraum erfolgte eine grundlegende Umgestaltung des europäischen (EU), deutschen und hessischen Datenschutzrechts. Am 25.05.2018, dem Tag, an dem die Datenschutz-Grundverordnung (DS-GVO) Geltung erlangte, begann laut Selmayr/Ehmann eine neue Zeitrechnung (DS-GVO Kommentar, 2. Aufl. 2018, Einführung Rdnr. 1). Selbst wenn man das für übertrieben hält, ist doch bemerkenswert, dass an diesem Tag die DS-GVO und die EU-Richtlinie für Justiz und Inneres (JI-Richtlinie; JI-RL) von einer breiteren Öffentlichkeit überhaupt erst und zudem überwiegend skeptisch zur Kenntnis genommen wurden. Die Skepsis beruht vor allem darauf, dass nicht nur einzelne Bestimmungen der DS-GVO, sondern generell die Anforderungen des Datenschutzrechts missverstanden wurden. Die JL-RL blieb weithin unbekannt.

1.2
Konsequenzen für die Berichterstattung

Dadurch wird auch die Aufgabenstellung der Datenschutz-Aufsichtsbehörden einschließlich der jährlichen Berichterstattung berührt. Bis zum 24.05.2018 waren die Aufgaben des Hessischen Datenschutzbeauftragten (HDSB) in § 24 HDSG 1999 geregelt.

§ 24 HDSG 1999

(1) Der Hessische Datenschutzbeauftragte überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den datenverarbeitenden Stellen. Zu diesem Zwecke kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er die Landesregierung und einzelne Minister sowie die übrigen datenverarbeitenden Stellen in Fragen des Datenschutzes beraten. Die Gerichte unterliegen der Kontrolle des Hessischen Datenschutzbeauftragten, soweit sie nicht in richterlicher Unabhängigkeit tätig werden. Der Hessische Datenschutzbeauftragte kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich und soweit sie sich nach § 4 Abs. 3 Satz 1 seiner Kontrolle unterworfen haben.

(2) Der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der datenverarbeitenden Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen

Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

…

Ab 25.05.2018 ergeben sich die Aufgaben der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit aus § 13 HDSIG.

§ 13 HDSIG

(1) Die oder der Hessische Datenschutzbeauftragte überwacht bei den öffentlichen und nicht öffentlichen Stellen sowie deren Auftragsverarbeitern die Anwendung dieses Gesetzes, der Verordnung (EU) Nr. 2016/679 und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften.

(2) Neben den Aufgaben nach Art. 57 der Verordnung (EU) Nr. 2016/679 hat die oder der Hessische Datenschutzbeauftragte die Aufgaben,

1. *die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,*
2. *die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder und Jugendliche besondere Beachtung finden,*
3. *den Landtag, die im Landtag vertretenen Fraktionen, die Landesregierung, die Kommunen und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,*
4. *die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie(EU) Nr. 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten bei der Verarbeitung personenbezogener Daten zu sensibilisieren,*
5. *auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,*
6. *sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Art. 55 der Richtlinie (EU) Nr. 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,*
7. *mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,*

8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,

9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und

10. Beratung in Bezug auf die in § 64 genannten Verarbeitungsvorvorgänge zu leisten.

Im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 nimmt die oder der Hessische Datenschutzbeauftragte zudem die Aufgaben nach § 52 Abs. 7 auch in Verbindung mit § 51 Abs. 4, § 53 Abs. 7 und § 55 wahr.

(3) Die oder der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, insbesondere ob diese zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung oder zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Sie oder er soll Maßnahmen anregen, die geeignet erscheinen, derartige Auswirkungen zu verhindern.

…

Die gegenüber der Öffentlichkeit bestehende Sensibilisierungs- und Aufklärungsaufgabe ist ausdrücklich als Rechtspflicht ausgestaltet (§ 13 Abs. 2 Nr. 2 HDSIG). Schon nach früherem Recht hatte der HDSB jährlich einen schriftlichen Tätigkeitsbericht vorzulegen. Dies ergab sich aus § 30 HDSG.

§ 30 Abs. 1 HDSG 1999

Zum 31. Dezember jeden Jahres hat der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis seiner Tätigkeit nach § 24 Abs. 1 bis 3 vorzulegen. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 10 und regt Verbesserungen des Datenschutzes an. Zwischenberichte sind zulässig. Gleichzeitig mit dem Bericht nach Satz 1 legt der Hessische Datenschutzbeauftragte dem Landtag einen Bericht über seine Tätigkeit nach § 24 Abs. 4 vor.

Die Berichtspflicht der oder des HBDI ist nunmehr in § 15 HDSIG geregelt.

§ 15 Abs. 3 HDSIG

Zum 31. Dezember jedes Jahres hat die oder der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis ihrer oder seiner Tätigkeit vorzulegen und regt Verbesserungen des Datenschutzes an. Die oder der Hessische Datenschutzbeauftragte macht diesen Bericht der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich. Zwischenberichte zur Vorlage bei dem Landtag und der Landesregierung sind zulässig.

Adressaten des Tätigkeitsberichtes waren bisher allein Landtag und Landesregierung. Diese sind weiterhin Primäradressaten der Berichte. Die Berichte sind nunmehr aber auch der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss „zugänglich zu machen". Deren ausdrückliche Erwähnung macht sie zu Sekundäradressaten, die nicht nur als Nichtbetroffene über Rechtsbeziehungen Dritter zu informieren, sondern inhaltlich-funktionell zu berücksichtigen sind. Für den Europäischen Datenschutzausschuss liegt das auf der Hand. Für seine Aufgabenerfüllung ist aus der Natur der Sache die nationale Berichterstattung unverzichtbar. Die Europäische Kommission kann den einheitlichen Vollzug der DS-GVO nur effektiv überwachen, wenn ihr aussagekräftige Berichte der nationalen Aufsichtsbehörden vorgelegt werden. Die Verpflichtung des oder der HBDI, die DS-GVO der Öffentlichkeit auch im Rahmen der Berichterstattung nahezubringen, ergibt sich letztlich aus dem Gebot einer effektiven Aufgabenerfüllung.

Die zum 25.05.2018 eingetretene Funktionserweiterung des Tätigkeitsberichtes gibt Anlass, die Rechtslage vor und ab Geltung der DS-GVO getrennt zu behandeln (Ziff. 3 und 4). Inhaltlich kommt Folgendes hinzu: Die Aufgabe, im Tätigkeitsbericht Missverständnissen des Datenschutzrechts entgegenzuwirken, ergab sich auch ohne einfachgesetzliche Regelung aus der verfassungsrechtlich, insbesondere rechtsstaatlich begründeten Sonderstellung der unabhängigen staatlichen (Datenschutz-)Aufsichtsbehörden. Das novellierte Datenschutzrecht enthält nur punktuelle gesetzliche Konkretisierungen dieser Sonderstellung, sodass die verfassungsrechtliche Fundierung eine Aufgabe von Wissenschaft und Praxis bleibt. Auch die Tätigkeitsberichte haben zur Bewältigung dieser Aufgabe beizutragen. Das geschieht im vorliegenden Tätigkeitsbericht in der Weise, dass der eigentliche Berichtsteil des Tätigkeitsberichtes um allgemeine Ausführungen zum Verständnis und zur Auslegung der DS-GVO erweitert wird. Dies entspricht der mit dem 35. Tätigkeitsbericht begonnenen Übung, den dargestellten konkreten Aufsichtstätigkeiten generelle Vorbemerkungen zum Stand des Datenschutzes und des Datenschutzrechts voranzustellen. Behandelt wurden bislang etwa die Funktion des Datenschutzes im Rahmen der nationalen Verfassungsordnung und des Unionsrechts (35. Tätigkeitsbericht, S. 21 ff.; 36. Tätigkeitsbericht, S. 21 f.; 38. Tätigkeitsbericht, S. 21 ff.), die Stoßrichtungen des Datenschutzes und sein Verhältnis zur Informationsfreiheit (37. Tätigkeitsbericht, S. 23 f.), die Konzeption der informationellen Selbstbestimmung (38. Tätigkeitsbericht, S 21 f.; 45. Tätigkeitsbericht, S. 21 f.), die Aufgabenstellung der Datenschutzbeauftragten nach nationalem Recht und nach Maßgabe des Unionsrechts (Unabhängigkeit) (36. Tätigkeitsbericht, S. 20 ff.; 41. Tätigkeitsbericht. S. 35 ff.; 43. Tätigkeitsbericht, S. 23 ff.), die spezifische Rolle Hessens bei der Fortentwicklung des Datenschutzrechts (39. Tätig-

keitsbericht S. 23 ff.; 40. Tätigkeitsbericht, S. 29 ff.), die Europäisierung des Datenschutzrechts (41. Tätigkeitsbericht, S. 32 ff.; 43. Tätigkeitsbericht, S. 27 ff.; 44. Tätigkeitsbericht, S. 21 ff.) und die internationalen Bezüge des Datenschutzrechts (42. Tätigkeitsbericht, S. 25 ff.; 43. Tätigkeitsbericht, S. 23 ff.). Im 46. Tätigkeitsbericht (S. 23 ff.) wurde im Vorgriff auf die zu erwartende Entwicklung der Handel mit personenbezogenen Daten thematisiert. Der von der Kommission betriebene Ausbau einer europäischen Datenwirtschaft (vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau eines gemeinsamen europäischen Datenraums" [SWD(2018) 125 final] vom 25.04.2018 (BRDrucks. 156/18) sowie Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zur „Mitteilung der Kommission an das EU-Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Aufbau einer europäischen Datenwirtschaft" [COM(2017) 9 final] bezieht sich zwar nur auf nichtpersonenbezogene Daten und soll die DS-GVO unberührt lassen (vgl. die Veröffentlichung der EU-Kommission: Enter the data economy, EU policies for a thriving data ecosystem, Issue 21 / 11.01.2017). Diese Beschränkung wird aber im Zeitalter von Ubiquitous Computing und Big Data auf längere Sicht nicht möglich sein und ist auch nicht erstrebenswert. Das Recht muss mit der technischen Entwicklung Schritt halten (vgl. bereits Ronellenfitsch, DVBl. 1989, 851 ff.). Die Reform des Datenschutzrechts ist deshalb eine Daueraufgabe. Bevor man jedoch weitere Reformvorhaben in Angriff nimmt, sollte man der DS-GVO die Chance geben, die ihr im Gesamtkomplex des Datenschutzrechts zukommende Wirksamkeit zu entfalten. Die Tragweite des aktuellen Umbruchs wird sich erst im Normvollzug erweisen. Ein rechtlich korrekter Normvollzug setzt Klarheit über die Regelungsreichweite voraus, die methodisch nachvollziehbar zu bestimmen ist.

1.3 Normvollzug

1.3.1 Regelungsreichweite der DS-GVO

Die DS-GVO hat schon auf Grund ihres Regelungscharakters als unmittelbar geltender Rechtsakt (Art. 288 Abs. 2 AEUV) einen umfassenden Geltungsanspruch. Hinzu kommt das Anliegen der Normadressaten und -anwender, möglichst alle datenschutzrechtlichen Regelungen in einem einheitlichen Gesetz aufzufinden. Schließlich wurden auch in diesem Zusammenhang einfache und verständliche Regelungen gewünscht. Die EU-Kommission strebte dementsprechend eine Vollharmonisierung an. Diese Zielsetzun-

gen hätten eine allumfassende unionsrechtliche Kodifikation erfordert. Dem entspricht die DS-GVO jedoch nicht und konnte dem nicht entsprechen: Erstens gilt für die Abgrenzung der Zuständigkeiten der Union der Grundsatz der begrenzten Einzelermächtigung (Art. 5 Abs. 1 S. 1 EU). Der Datenschutz erstreckt sich indessen auch auf Bereiche, in denen keinerlei Zuständigkeiten der EU bestehen. Hier sind in Deutschland allein der Bund oder die Länder zuständig. Zweitens wird das Unionsrecht von Organen der Mitgliedstaaten vollzogen, denen allein die Zuständigkeit zur Regelung der nationalen Verwaltungsorganisation und des Verwaltungsverfahrens obliegt. Drittens sind die Lebensumstände in der globalisierten vernetzten Informationsgesellschaft derart komplex, dass einfache Regelungen ausscheiden. So bereiten etwa mehrpolige Rechtsverhältnisse Schwierigkeiten, die nur durch diffizil abgewogene Problemlösungen zu bewältigen sind. Der Gesetzgeber kann dann zwar sprachlich einfache und „schlanke“ Regelungen treffen, die differenzierte Problemlösung verlagert sich dadurch aber nur in den Normvollzug. Die Normierung unbestimmter Rechtsbegriffe und Eröffnung von Ermessens- und Abwägungsspielräumen ist aber im (föderalen) Verfassungsstaat nur begrenzt möglich (Stichwort: „Wesentlichkeitstheorie“), wenn auch einzuräumen ist, dass systematisch strukturierte Kodifikationen kohärente Auslegungen erleichtern. Das Zeitalter für einfachgesetzliche, in sich stimmige und aus sich selbst heraus verständliche, schlichte Kodifikationen ist gleichwohl unwiederbringlich vorüber (vgl. Lepsius JuS 2019, 14 ff.). Die tatsächlichen Verhältnisse bei der Datenverarbeitung sind so kompliziert geworden und wandeln sich so schnell, dass der Gesetzgeber ständig zum Nachbessern gezwungen ist. All dies zusammengenommen erklärt, warum die DS-GVO nicht nur Spezifizierungsklauseln, sondern auch zahlreiche echte Öffnungsklauseln enthält, die ergänzende und abweichende Regelungen durch die Mitgliedstaaten erlauben und erfordern (hierzu Ziff. 2). Im Geltungsbereich der DS-RL gilt das ohnehin.

1.3.2
Auslegung von Unionsrecht

Die Auslegung von Rechtsvorschriften erfolgt in allen Mitgliedstaaten der EU nach subjektiven und objektiven Kriterien, die Wortlaut, Regelungszusammenhang, Regelungswille sowie Regelungszweck betreffen. Im Anschluss an Savigny (System des heutigen römischen Rechts I, 1840, S. 213 f.) werden grammatikalische, historische, systematische und teleologische Kriterien der Auslegung unterschieden. Die Kriterien ergänzen sich zumeist, können aber auch kollidieren. Vor allem unterscheidet sich das Gewicht der jeweiligen Auslegungskriterien in den einzelnen Rechtsordnungen der EU-Mitgliedstaaten.

Das darf jedoch nicht zu einer uneinheitlichen Anwendung des Unionsrechts führen. Der EuGH betrachtete daher schon zu Beginn seiner Spruchtätigkeit die europäische Staatenverbindung als eigenständige Rechtsordnung und praktizierte eine autonome Auslegung des seiner Deutungshoheit unterliegenden Rechts (EuGH Slg. 1982, 12). Für die Auslegung des Unionsrechts kommt es hiernach zunächst auf den Wortlaut der streitgegenständlichen Bestimmung an. Zu berücksichtigen und zu vergleichen sind alle Sprachfassungen (EuGH Slg. 1983, 3781, Rdnr. 12), was die Wortinterpretation relativiert. Sie ist gleichwohl Ausgangspunkt jeglicher Auslegung, da Gesetzestexte nur in Sprachform (im Wortsinn) denkbar sind. Bei eindeutigem Wortlaut gilt die „acte-clair-" bzw. „acte-eclairé-Doktrin", wonach dem EuGH eine Rechtsfrage dann nicht vorzulegen ist, wenn die Auslegung vernünftigerweise keine Zweifel aufkommen lässt (EuGH Slg. 1982, 3415 Rdnr. 23 ff., vgl. auch BVerfG, NJW 2018, 656 Rdnr. 43). Der historischen Auslegung kommt beim Unionsrecht keine maßgebliche Bedeutung zu. Beim Primärrecht ist eine aussagekräftige Erforschung der Willensbildung der Vertragsparteien kaum möglich. Beim Sekundärrecht ist die Willensbildung der Gesetzgebungsorgane nur zu berücksichtigen, soweit subjektive Vorstellungen in den Gesetzestext Eingang gefunden haben. Die Begründung für die gesetzliche Regelung findet sich in den Erwägungsgründen, die unmittelbar zur Gesetzesauslegung herangezogen werden können (EuGH Slg. 1997, I-2549 Rdnr. 21). Die systematische Auslegung stellt auf den Kontext der Einzelnorm innerhalb der Gesamtregelung ab, klärt das Verhältnis der einzelnen Artikel untereinander, zieht Folgerungen aus der Positionierung der Vorschrift und deckt Regelungslücken auf. Im Unionsrecht ist eine wichtige Unterkategorie der systematischen Auslegung die primärrechtskonforme Auslegung des Sekundärrechts. Die teleologische Auslegung schließlich fragt nach Sinn oder Zweck einer Regelung. Bei der Auslegung von Unionsrecht kommt der Zweckgedanke in zweifacher Hinsicht zum Tragen: Zum einen spielt bei der Bewertung eines Rechtsakts seine in den Erwägungsgründen begründete konkrete Zwecksetzung eine Rolle. Die Auslegung soll dazu beitragen, die Legitimität, Kompetenz und Verhältnismäßigkeit des Rechtsakts zu gewährleisten. Zum anderen dient die teleologische Methode dazu, den Integrationsprozess allgemein zu fördern, in Gang zu halten und zu bewahren (integrationssichernde Auslegung).

2. Rechtsentwicklung

2.1
Europäische Union

Auf der EU-Ebene konzentrierten sich die Bemühungen im Berichtszeitraum auf die möglichst einheitliche Geltung und den einheitlichen Vollzug der DS-GVO. Die Kommission erließ zu diesem Zweck bereits am 24.01.2018 die Mitteilung an das Parlament und den Rat „Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung ab 25.05.2018 [COM(2018) 43 final]". Daneben ergingen Rechtsakte, die zwar Spezifizierungs- und Öffnungsklauseln ausfüllen oder bereichsspezifisches Datenschutzrecht enthalten, an der datenschutzrechtlichen Konzeption der DS-GVO – insbesondere an den Grundsätzen der Art. 5 ff. DS-GVO – jedoch nichts ändern. Zu nennen sind etwa

– der Beschluss (EU) 2018/893 des Rates vom 18.06.2018 über den Standpunkt, der im Namen der Europäischen Union im Gemeinsamen EWR-Ausschuss zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 mit der Liste gemäß Art. 101 des EWR-Abkommens zu vertreten ist (Datenschutz-Grundverordnung) (ABl. L 159 vom 22.06.2018 S. 31 ff.);
– die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23.10.2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) 45/2001 und des Beschlusses 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39 ff.)
– sowie die Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28.11.2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 07.12.2018, S. 56 ff.).

2.2
Mitgliedstaaten

Die Ergänzungsbedürftigkeit der DS-GVO wird von der Kommission und in den Mitgliedstaaten unterschiedlich gesehen. Soweit ersichtlich, fand

die intensivste Diskussion der kompetenzrechtlichen Voraussetzungen des Unionsrechts in der Bundesrepublik Deutschland statt. Hier, im Bund und in den Ländern, wurden folgerichtig die ersten, die DS-GVO ergänzenden, Ausführungsgesetze erlassen (vgl. Ziff. 2.3 und 2.4). Einzelne Mitgliedstaaten halten dagegen offenbar Durchführungsgesetze für überflüssig. Zumeist befinden sich Durchführungsgesetze in Vorbereitung. In folgenden Mitgliedstaaten der EU ergingen bislang wie in Deutschland ebenfalls Durchführungsgesetze zur DS-GVO (Überblick bei Pohle, Cri 2018, 97 ff., 133 ff.; ferner DS-GVO-Umsetzung: Aktueller Gesetzesstand der EU-Mitgliedsländer – ISiCO Datenschutz https://www.isico-datenschutz.de/.../dsgv...: Die DS-GVO in den EU-Mitgliedsländern: Wie ist der Stand? – Schürmann Rosenthal Dreyer Rechtsanwälte https://www.srd-rechtsanwaelte.de/.../...):

Belgien: Gesetz vom 03.12.2017 über die Errichtung einer Aufsichtsbehörde „Loi du 03 décembre 2017 portant création de l'Autorité de protection des données"/„Wet tot oprichting van de Gegevensbeschermingsautoriteit" (Moniteur Belge/Belgisch Staatblad vom 10.01.2018 S. 989). Das Gesetz beschränkt sich auf die Errichtung der Aufsichtsbehörde (Autorité de protection des données" – APR), welche an die Stelle der Kommission zum Schutz der Privatsphäre („Commission de la protection de la vie privée" – CPVP) trat.

Dänemark: Gesetz über ergänzende Bestimmungen für eine Verordnung über den Schutz von Personen in Bezug auf die Verarbeitung personenbezogener Daten und über den freien Verkehr solcher Daten – Datenschutzgesetz „Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger – databeskyttelsesloven" vom 17.05.2018 (Justitsmin., j.nr. 2017-7910-0004). Das Gesetz enthält weitergehende Regelungen als die DS-GVO etwa bei der Datenverarbeitung durch Arbeitnehmer.

Frankreich: Gesetz zum Schutz personenbezogener Daten „Loi n° 2018-493 relative à la protection des données personnelles du 20.06.2018 (NOR: JUSC1732261L). Das Gesetz erklärt sich rückwirkend zum 25.05.2018, wiederholt und konkretisiert zahlreiche Bestimmungen der DS-GVO und bestimmt die Aufgaben und Befugnisse der Nationalen Kontrollbehörde Frankreichs CNIL (Commission Nationale de l'Informatique et des Libertés).

Irland: Datenschutzgesetz 2018 „Data Protection Bill 2018" vom 18.05.2018 (Irishstatutebook07). Das Gesetz enthält eine Vielzahl differenzierender Regelungen, die bei konsequentem Vollzug der Tauglichkeit Irlands als Datenschutz-Fluchtburg für internationale Technologiekonzerne entgegenstehen.

Kroatien: Gesetz über die Umsetzung allgemeiner Datenschutzvereinbarungen DS-GVO-Umsetzungsgesetz „ZAKONO PROVEDBI OPĆE UREDBE O ZAŠTITI PODATAKA“ vom 27.04.2018 (Amtsblatt NN24/2018). Das Gesetz enthält weitgehende Parallelregelungen zur DS-GVO.

Lettland: Das Gesetz zur Verarbeitung personenbezogener Daten „Personas datu apstrādes likums“ vom 02.04.2018 (12 Saeima, Nr. 1182/Lp 12) übernimmt weitgehend die DS-GVO, die sie um zwei Legaldefinitionen erweitert. Ferner wird die Behörde des lettischen Datenschutzinspektors eingerichtet.

Niederlande: Beschluss vom 16.05.2018 über das Inkrafttreten des Gesetzes über den allgemeinen Datenschutz „Besluit van 16 mei 2018 tot vaststelling van het tijdstip van inwerkingtreding van de Uitvoeringswet Algemene verordening gegevensbescherming“ (Staatsblad 2018, 145) Die Allgemeine Datenschutzverordnung „Uitvoeringswet Algemene verordening gegevensbescherming“ erweitert unter Berufung auf Art. 9 DS-GVO die Ausnahmen vom grundsätzlichen Verbot der Verwendung von personenbezogenen Daten, erlaubt es aber zugleich unter bestimmten Voraussetzungen, Daten dritter Personen zu erheben, sofern dies erforderlich ist oder ein verhältnismäßiges Interesse besteht. Datenschutzbehörde ist die Autoriteit Persoonsgegevens.

Österreich: Das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG; BGBl. I Nr. 165/1999), das durch mehrere Anpassungsgesetze konkretisiert und stark verändert wurde. Eine zusammenfassende Regelung enthält das Datenschutz-Anpassungsgesetz 2018 (BGBl. I Nr. 120/2017). Der Titel lautet nicht mehr „Datenschutzgesetz 2000“ (DSG 2000), sondern nur noch „Datenschutzgesetz“ (DSG). Die Änderungen sind so umfangreich, dass fast alle Verweise auf Bestimmungen des DSG 2000 nicht mehr gültig sind. Die Neufassung des DSG erfolgte nach Ablauf des Berichtszeitraums.

Rumänien: Gesetz Nr. 190 zur Änderung und Fertigstellung des Gesetzes Nr. 102/2005 über die Einrichtung, Organisation und den Betrieb der nationalen Aufsichtsbehörde für die Verarbeitung personenbezogener Daten und für die Aufhebung des Gesetzes Nr. 1 677/2001 (Proiect de Lege pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum) vom 31.07.2018. Die Öffnungsklauseln der DS-GVO wurden genutzt, um Ausnahmen für öffentliche Behörden, politische Parteien u. a. festzulegen.

Schweden: Neues Datenschutzgesetz (Ny Dataskyddslag) vom 18.04.2018 (Riksdagens protokoll 2017/18:100). Das Gesetz macht von der Möglichkeit nach Art. 85 DS-GVO Gebrauch, der Meinungs- und Informationsfreiheit in der Abwägung mit dem Datenschutz größeres Gewicht beizumessen.

Slowakei: Das „Neue Datenschutzgesetz“, d. h. das „Gesetz über den Schutz personenbezogener Daten und die Änderung bestimmter Gesetze“ (Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov) Nr. 18 vom 01.01.2018 in Abänderung des Gesetzes No. 122/2013 über den Datenschutz Nr. 18/2018.

Ungarn: Das Informationsfreiheitsgesetz von 2011 wurde durch zwei Ergänzungen an die DS-GVO angepasst. Das erste Ergänzungsgesetz betrifft die Einrichtung einer Datenschutzbehörde. Das zweite Ergänzungsgesetz enthält Abweichungen von der DS-GVO. Die nationale Datenschutzbehörde heißt „Nemzeti Adatvédelmi és Információszabadság Hatóság“ (NAIH).

2.3
Deutschland

Auf das DSAnpUG-EU, welches das BDSG 2017 ersetzte, wurde bereits im 46. Tätigkeitsbericht (Ziff. 1.2.3) hingewiesen. Durch den Entwurf zum 2. DSAnpUG-EU (BTDrucks. 19/4674) soll das 1. DSAnpUG-EU nachgebessert werden, um die grund- und europarechtlichen Vorgaben zu erfüllen.

Hierbei sieht der Referentenentwurf Änderungen bei folgenden Normen des BDSG vor:

– § 4 BDSG – Videoüberwachung öffentlich zugänglicher Räume
– § 9 BDSG – Zuständigkeit
– § 16 BDSG – Befugnisse
– § 22 BDSG – Verarbeitung besonderer Kategorien personenbezogener Daten
– § 86 BDSG (Neueinführung) – Verarbeitung personenbezogener Daten für Zwecke staatlicher Auszeichnungen und Ehrungen

Auch die Länder passten ihre Datenschutzgesetze an die DS-GVO an:

Baden-Württemberg: Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/67 (GBl. 2018, S. 173)

Bayern: Bayerisches Datenschutzgesetz (BayDSG) vom 15.05.2018 (GVBl. 2018, S. 230)

Brandenburg: Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz – BbgDSG) vom 08.05.2018 (GVBl. I/18, [Nr. 7])

Berlin: Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG) vom 13.06.2018 (GVBl. 2018, S. 418)

Bremen: Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) vom 08.05.2018 (Brem. GBl. 2018, S. 131)

Hamburg: Hamburgisches Datenschutzgesetz (HmbDSG) vom 18.05.2018 (HmbGVBl. 2018, S. 145

Hessen: vgl. Ziff. 2.4

Mecklenburg-Vorpommern: Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 22.05.2018 (GVBl. 2018, S. 194)

Niedersachsen: Niedersächsisches Datenschutzgesetz (NDSG) vom 16.05.2018 (Nds. GVBl. 2018, S. 66)

Nordrhein-Westfalen: Datenschutzgesetz Nordrhein-Westfalen vom 17.05.2018 (GV. NRW. 2018, S. 244, ber. S. 278 und S. 404)

Rheinland-Pfalz: Landesdatenschutzgesetz (LDSG) vom 08.05.2018 (GVBl. 2018, S. 53)

Saarland: Saarländisches Datenschutzgesetz vom 16.05.2018 (Amtsbl. 2018 I, S. 254)

Sachsen: Sächsisches Datenschutzgesetz vom 25.08.2003 (Sächs. GVBl. S. 330), zuletzt geändert durch Art. 46 des Gesetzes vom 26.04.2018 (Sächs. GVBl. 2018, S. 198)

Sachsen-Anhalt: Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt – DSG LSA) i. d. F. der Bekanntmachung vom 13.01.2016 (GVBl. LSA 2016, S. 24), zuletzt geändert durch Art. 1 des Gesetzes vom 21.02.2018 (GVBl. LSA 2018, S. 10)

Schleswig-Holstein: Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) vom 02.05.2018 (GVOBl. 2018, S. 162)

Thüringen: Thüringer Datenschutzgesetz (ThürDSG), verkündet als Art. 1 des Thüringer Gesetzes zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 06.06.2018 (GVBl. 2018, S. 229)

2.4
Hessen

In Hessen erfolgte die Novellierung des Landesdatenschutzrechts durch das Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 und zur Informationsfreiheit vom 03.05.2018 (GVBl. 2018, S. 82). Das Gesetz ist in Artikel untergliedert; es ist somit ein Artikelgesetz. Bei den Artikelgesetzen sind zu unterscheiden „Omnibusgesetze", bei denen unterschiedliche Regelungsbereiche in einem einzigen Gesetz zusammengefasst und innerhalb des Gesetzes durch Artikel voneinander abgehoben werden (vgl. Lachner, Das Omnibusgesetz, 2007, pass.), und Änderungsfolgegesetze, bei denen eine bestimmte neu geregelte Thematik zu Änderungen in zahlreichen Fachgesetzen führt. Omnibusgesetze werden jeweils für sich ausgelegt. Änderungsfolgegesetze machen es dagegen erforderlich, jeweils den gemeinsamen Nenner herauszuarbeiten. Titel, Gliederung und Entstehungsgeschichte des HDSIG vermitteln den Eindruck eines Omnibusgesetzes. Der vollständige Titel des HDSIG führt drei gesonderte Regelungsbereiche auf, die nicht zwingend eine Regelungseinheit erfordern. Auch der Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein hessisches Gesetz zur Anpassung des hessischen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 und zur Informationsfreiheit behandelt die Anpassung des hessischen Landesrechts an die VO 2016/79, die Umsetzung der RL 2016/79 und die Informationsfreiheit als unterschiedliche Materien. Aber schon bei den die Fachgesetze betreffenden Folgeänderungen geht das Gesetz von der Einheitlichkeit des Datenschutzrechts aus. Unterschiedliche Zielsetzungen wurden dagegen für den Datenschutz und die Informationsfreiheit angenommen (LTDrucks. 19/5728); genauer: Das Datenschutzrecht wurde lediglich als Schranke der Informationsfreiheit verstanden. In der Entwurfsbegründung heißt es hierzu:

„Die Bürgerinnen und Bürger in Hessen erhalten einen gesetzlichen Anspruch auf Zugang zu den bei öffentlichen Stellen des Landes vorhandenen amtlichen Informationen. Dabei bleibt nicht nur der Schutz von Betriebs- oder Geschäftsgeheimnissen gewährleistet, sondern insbesondere auch von personenbezogenen Daten. Aufgrund des engen Zusammenhangs zwischen dem Informationszugangsrechts auf der einen Seite und dem Datenschutz auf der anderen Seite werden die Regelungen zum Informationszugang als weiterer Teil in das Hessische Datenschutz- und Informationsfreiheitsgesetz eingefügt."

Im Zuge des Gesetzgebungsverfahrens setzt sich jedoch die Auffassung durch, dass Datenschutz und Informationsfreiheit keine Gegensätze, sondern

Elemente einer umfassend verstandenen informationellen Selbstbestimmung sind. Datenschutz und Informationsfreiheit wurden daher nicht in mehreren Artikeln, sondern in einem Artikel untergebracht. Damit verfügt Hessen über das modernste Datenschutzgesetz der deutschen Ausführungsgesetze. Das Verständnis der Informationsfreiheit als dem Datenschutz korrespondierendes Element der informationellen Selbstbestimmung ist aber noch nicht in das allgemeine Bewusstsein eingedrungen. Daher wird noch auf die jüngste Entwicklung der informationellen Selbstbestimmung im Zusammenhang mit der Informationsfreiheit zurückzukommen sein. Im Zusammenhang mit dem herkömmlichen Datenschutz genügt der Hinweis, dass das HDSIG vom Hessischen Landtag am 26.04.2018 in dritter Lesung verabschiedet wurde. Mit Gesetz vom 12.09.2018 wurde mit Art. 5 das HDSIG um zwei Vorschriften ergänzt, die sich auf die Datenverarbeitung bei öffentlichen Ehrungen und Gnadenverfahren beziehen.

2.5
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung hat im laufenden Jahr einige Änderungen erfahren. Neben den notwendigen Umsetzungen aufgrund der Europäischen Datenschutzreform war Anlass die Rechtsprechung des BVerfG zum BKA-Gesetz sowie das Anliegen der Regierungsfraktionen, weitere Ermächtigungsgrundlagen für die Polizei zu schaffen. Nicht in allen Punkten ist es dabei gelungen, die Verhältnismäßigkeit zu wahren.

Zum Ablauf der Gesetzgebungsverfahren

Die zum Teil umfassenden Änderungen im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) – soweit diese auch datenschutzrechtlich relevant sind – beruhten auf drei Umständen:

– Im HSOG mussten die Vorgaben der JI-Richtlinie (Richtlinie 2016/680 vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten) umgesetzt werden.
– Das BVerfG hatte 2016 in seiner Entscheidung zum BKA-Gesetz (1 BvR 966/09, 1 BvR 1140/09; BVerfGE 141, 220-378) Rahmenbedingungen formuliert, die auch für die Landespolizeigesetze relevant sind.

– Die Regierungsfraktionen hatten sich entschieden, zusätzliche Ermächtigungsgrundlagen insbesondere zur Bekämpfung des Terrorismus für die Polizei zu schaffen.

Die einzelnen Änderungen waren zum Teil im Ablauf schwierig nachzuvollziehen, da sie in zwei gleichzeitig zu beratenen Gesetzgebungsvorhaben enthalten waren. Zum einen war dies der Art. 18 des Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit, das als Entwurf der Regierungsparteien am 05.12.2017 in den Landtag eingebracht wurde (LTDrucks. 19/5728). Weitere – nicht unwesentliche – Änderungen enthielt der Gesetzentwurf der Regierungsfraktionen zur Neuregelung des Verfassungsschutzes in Hessen (LTDrucks. 19/4512 vom November 2017).

Umsetzung der BKA-Gesetz-Entscheidung des BVerfG

In der genannten Entscheidung hat das BVerfG 2016 neu definiert, unter welchen Voraussetzungen die Polizei Daten, die zu einem Zweck berechtigt erhoben und verarbeitet werden durften, auch für weitere Zwecke nutzen darf. Dazu hat es den Begriff der hypothetischen Neuerhebung geprägt. Diese würde die Verhältnismäßigkeitsanforderungen für eine Zweckänderung konkretisieren. Voraussetzung für eine Zweckänderung sei danach aber, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Nicht in jedem Fall identisch seien die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmten unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig entsprechend auch ausreichend, sei insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergebe.

Der Gesetzgeber kann danach eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht

drohenden Gefahren für vergleichbar gewichtige Rechtsgüter ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist.

Die nunmehr neugefassten Regelungen zur Datenerhebung im HSOG lassen die Weiterverarbeitung personenbezogener Daten zur Erfüllung der Aufgaben der Gefahrenabwehr- und Polizeibehörden zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, nur zu, wenn mindestens vergleichbar gewichtige Straftaten oder Ordnungswidrigkeiten verhütet oder mindestens vergleichbar gewichtige Rechtsgüter oder sonstige Rechte geschützt werden sollen und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung solcher Straftaten ergeben oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für solche Rechtsgüter oder sonstige Rechte erkennen lassen, zu deren Schutz die entsprechende Datenerhebung verfassungsrechtlich zulässig wäre. Damit sind auch nach meiner Einschätzung in diesem Kontext die vom BVerfG gesetzten Kriterien erfüllt.

Die weiteren Änderungen im HSOG, die mit der Umsetzung der Entscheidung zum BKA-Gesetz begründet worden sind, können hier nicht im Einzelnen dargestellt werden. Allerdings sehe ich auch keinen Grund, insoweit Bedenken zu formulieren.

Erweiterte Erhebungsbefugnisse – QuellenTKÜ und Online-Durchsuchung

Die Voraussetzungen für die Online-TKÜ in § 15a HSOG wurden erweitert. Zusätzlich wurde auch die sog. Online-Durchsuchung neu aufgenommen. Diese Änderungen waren ursprünglich im Gesetzentwurf für das HSOG nicht vorgesehen. Allerdings waren entsprechende Befugnisse für den Verfassungsschutz vorgesehen. Diese Regelungen wurden im Rahmen der Landtagsanhörung und auch in der öffentlichen Debatte in großem Umfang kritisiert.

Als Resonanz darauf haben die Regierungsfraktionen von entsprechenden Befugnissen für den Verfassungsschutz abgesehen und insoweit ihren Gesetzesvorschlag zurückgezogen. Im Rahmen dieser Aktion wurde dann jedoch kurzfristig die entsprechende Änderung für das HSOG in den Landtag eingebracht. Eine echte Auseinandersetzung, ob und warum dies als polizeiliche Befugnisse erforderlich ist und inwieweit dazu im Interesse des informationellen Selbstbestimmungsrechts Rahmenbedingungen zu schaffen waren, konnte nicht erfolgen.

In der streitigen Debatte zum HVSG wurde insbesondere auf ein grundsätzliches Sicherheitsproblem hingewiesen. Um die notwendigen Tools zu entwickeln bzw. einem konkreten Einsatz anzupassen und auf dem zu

überwachenden Rechner zu implementieren, ist es notwendig, eine IT-Sicherheitslücke zu kennen. Diese sollten – sobald erkannt – eigentlich dem jeweiligen Software-Entwickler kommuniziert werden, damit sie schnellstmöglich durch entsprechende Updates geschlossen werden, um einen Schaden von allen Nutzern abzuwenden. Das Ausnutzen solcher Lücken und damit das notwendige Verschweigen durch den Staat ist problematisch. Damit toleriert er die Möglichkeit, dass andere – mit Schädigungsabsicht – diese Lücke ebenfalls nutzen.

Ob und wie diese Instrumentarien in Zukunft zum Einsatz kommen und inwieweit dabei die verfassungsrechtlichen Rahmenbedingungen für rechtmäßige Eingriffe in das Recht auf informationelle Selbstbestimmung gewahrt werden, wird sorgfältiger Begleitung bedürfen. Dies ist auch Gegenstand der neuen Prüfverpflichtung gemäß § 29a HSOG (vgl. dazu auch Ziff. 2.7)

Die Umsetzung der Europäischen Datenschutzreform

Nicht für alle Bereiche, in denen die Polizei präventiv tätig wird, ist der Anwendungsbereich der JI-Richtlinie eröffnet. Gemäß Art. 1 Abs. 1 ist vom Geltungsbereich der Schutz und die Abwehr von Gefahren für die öffentliche Sicherheit mitumfasst. Dies ist nicht deckungsgleich mit dem Geltungsbereich gemäß § 3 Abs. 1 HSOG.

Art. 1 Abs. 1 JI-Richtlinie

Diese Richtlinie enthält Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

§ 3 Abs. 1 HSOG

Die Vorschriften dieses Gesetzes finden Anwendung bei der Erfüllung von Aufgaben der Gefahrenabwehr und weiterer Aufgaben nach § 1. Vorschriften des Bundes- oder des Landesrechts, in denen die Gefahrenabwehr und die weiteren Aufgaben besonders geregelt sind, gehen diesem Gesetz vor. Soweit die besonderen Rechtsvorschriften keine abschließenden Regelungen enthalten, ist dieses Gesetz ergänzend anzuwenden.

Daher muss für eine Vielzahl von Regelungskomplexen differenziert werden, ob Regelungen der DS-GVO oder des HDSIG neben den bereichsspezifischen Regelungen des HSOG zur Anwendung kommen. Das Gesetz selbst definiert nicht, welche konkreten Aufgaben nicht vom Geltungsbereich der JI-Richtlinie umfasst sind, sondern verweist abstrakt jeweils auf den Anwendungsbereich des § 40 HDSIG, der jedoch insoweit nur den Wortlaut des Art. 1 JI-Richtlinie aufnimmt. Im Weiteren wird daher jeweils auf das HDSIG

oder die DS-GVO Bezug genommen. Damit sind die Vorschriften für die Anwender genauso wie für Bürgerinnen und Bürger deutlich schwieriger erschließbar als die bisherigen Regelungen des HSOG. Damit wird zum Teil sogar überdeckt, dass im Ergebnis sich keine Auswirkungen auf die Praxis ergeben, da der materielle Regelungsgehalt sich nicht geändert hat. Ob dies insgesamt noch als normenklare Regelung gelten kann – und damit eine wesentliche Voraussetzung für zulässige Eingriffe in das Recht auf informationelle Selbstbestimmung erfüllt –, muss auch die zukünftige Praxis zeigen.

Zuverlässigkeitsüberprüfungen

Im Rahmen der Möglichkeiten, Zuverlässigkeitsüberprüfungen durchzuführen, wurden mehrere Änderungen aufgenommen. Zum einen kann jetzt auch der Verfassungsschutz an diesen Verfahren beteiligt werden. Zusätzlich zur Befugnis für den Verfassungsschutz, Daten in diesem Zusammenhang übermitteln zu dürfen, wurde auch ein neuer Anlass definiert, wann eine solche Prüfung zulässig ist (zur Problematik dieser Regelung siehe Ziff. 2.6).

Eine Beteiligung des Verfassungsschutzes bei Zuverlässigkeitsüberprüfungen im Rahmen der §§ 13a und b soll erfolgen, soweit dies in Einzelfällen erforderlich ist. In der Praxis besteht hier noch erheblicher Bedarf, Kriterien dafür zu entwickeln, wann ein solcher Einzelfall vorliegt. Muss dies immer in der Person des Betroffenen begründet sein oder kann dies auch von der Art der Tätigkeit der zu überprüfenden Personen bzw. ihrem Einsatzort abhängig sein. Dies spielt insbesondere bei der weiteren Neuregelung eine Rolle. Gemäß § 13b Abs. 1 S. 3 kann nunmehr auch die Polizei anregen, dass im Kontext einer privaten Veranstaltung eine Zuverlässigkeitsüberprüfung stattfinden kann.

Eine wirkliche Konzeption oder gar Vorgaben von Seiten des Landespolizeipräsidiums, nach welchen Kriterien sowohl die Veranstaltung als auch eine Auswahl des zu überprüfenden Personenkreises getroffen werden kann, ist mir bis jetzt nicht bekannt.

Videoüberwachung

Die Regelungen zur Videoüberwachung im Rahmen der Gefahrenabwehr haben eine grundlegende Neuordnung gefunden. Dies ist auch im Kontext mit dem neugeschaffenen § 4 HDSIG zu sehen, der es nunmehr ausdrücklich öffentlichen Stellen ermöglicht, unter bestimmten Voraussetzungen – etwa zur Wahrung des Hausrechts – Videokameras einzusetzen. Damit ist gleichzeitig klargestellt, dass die Regelungen des HSOG in § 14 Abs. 3 und 4 nur im Kontext der klassischen Gefahrenabwehr zur Anwendung kommen können.

§ 14 Abs. 3 und 4 HSOG

(3) Die Gefahrenabwehr- und 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 sowie der Name und die Kontaktdaten der oder des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen. Abs. 1 Satz 2 und 3 gilt entsprechend.

(4) Die Gefahrenabwehr- und die Polizeibehörden können mittels Bildübertragung offen beobachten und aufzeichnen

1. *zum Schutz besonders gefährdeter öffentlicher Einrichtungen oder Räumlichkeiten,*
2. *zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.*

Soweit der Inhaber des Hausrechts nicht Gefahrenabwehr- oder Polizeibehörde ist, gilt er im Fall des Satz 1 Nr. 1 als Gefahrenabwehrbehörde. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 2 und 3 gelten entsprechend.

Nach dem Willen des Gesetzgebers gibt es nunmehr keine Unterscheidung mehr, ob die Polizei oder die Gefahrenabwehrbehörde – die Kommune – solche Anlagen betreiben will. Damit ist zwar die bisherige Unterscheidung aufgehoben, die die Errichtung für die Gefahrenabwehrbehörden an eine höhere Hürde geknüpft hatte, denn dort mussten schon entsprechende Straftaten vorgefallen und im Rahmen der Gefahrprognose auch weiterhin zu erwarten sein. Die jetzige Reglung greift allerdings die Realität auf. In der Mehrzahl der mir bekannten Fälle kam die Anregung für eine Überwachung aus den politischen Gremien der Kommune, wird aber von der Polizei durchgeführt und in dieser Konstellation von der Landesregierung auch durch nicht unerhebliche Zuschüsse gefördert. Faktisch wird dies daher nach meiner Einschätzung zu keinen wesentlichen Änderungen führen, ob im Einzelfall eine Videoüberwachungsanlage geplant bzw. umgesetzt wird oder nicht.

Die Neugestaltung des § 14 Abs. 4 greift Fragen aus der Praxis auf. Wiederholt sollte nicht eine besonders gefährdete Einrichtung insgesamt, sondern nur einzelne Räumlichkeiten innerhalb eines Gebäudes abgesichert werden. Genannt wurde etwa der Aufbewahrungsraum für Asservate wie Waffen und/oder Rauschmittel bei der Staatsanwaltschaft oder der Zugang zu Kassen- bzw. Tresorräumen. Dies ist auch aus meiner Sicht eine sinnvolle Klarstellung.

Da insgesamt am System der Videoüberwachung für öffentliche Stellen in Hessen erhebliche Änderungen vorgenommen wurden, hatte ich auch angeregt, zwei weitere Punkte aufzugreifen, die ich für missverständlich bzw. sogar eindeutig unverhältnismäßig halte.

Dies bezieht sich zunächst auf § 14 Abs. 3 S. 4, der auf § 14 Abs. 1 S. 2 und 3 verweist und damit eine Speicherdauer aller Aufnahmen von bis zu zwei Monaten ermöglicht. Dies ist unverhältnismäßig und entspricht auch nicht der allgemeinen Praxis. So empfiehlt selbst das LKA in einer Handreichung für die Kommunen nur eine Speicherdauer von bis zu zehn Tagen. Dieser Zeitraum ist völlig ausreichend, um zu entscheiden, ob eine Auswertung und ggf. eine Sicherung der entsprechenden aufgenommenen Sequenzen für weitere Maßnahmen oder ein einzuleitendes Strafverfahren erforderlich sind. Für diese dann so gesicherten Sequenzen gelten die allgemeinen Aufbewahrungsvorschriften für das jeweilige Verfahren. Damit ist eine Aufbewahrung aller Aufzeichnungen für einen derart langen Zeitraum nicht erforderlich.

Die Formulierung in Abs. 3 S. 3 hat zu Missverständnissen geführt. Sie war geschaffen worden, um eine regelmäßige Überprüfung der Rechtmäßigkeit des Betriebs einer Anlage zu erreichen. Dabei sollte sichergestellt werden, dass eine Anlage auch solange betrieben werden kann, bis diese Überprüfung zu einem negativen Ergebnis führt. Sollte sich jedoch im Laufe der 2-Jahres-Frist eindeutig ergeben, dass die Voraussetzungen an diesem Ort nicht mehr vorliegen, kann auf diese Weise die Rechtmäßigkeit einer Videoüberwachung nicht statuiert werden. Dies kommt etwa in Fällen in Betracht, wo durch Umgestaltung oder Bebauung eines Platzes sich die örtliche Situation so verändert, dass die ursprüngliche Gefahrenlage nicht mehr angenommen werden kann. Das muss besonders dann gelten, wenn von vornherein abzusehen ist, dass die Voraussetzungen für eine Videoüberwachung nur für einen bestimmten Zeitraum gegeben sind. So kann der Einsatz von Videotechnik für ein bestimmtes Ereignis – z. B. Großveranstaltungen wie der Hessentag – nicht eine Videoüberwachung für zwei Jahre rechtfertigen.

Deshalb hatte ich vorgeschlagen zu formulieren:

„Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen."
Der Gesetzgeber ist leider nur dem letzteren Vorschlag gefolgt.

Rahmen für den Einsatz neuer technischer Verfahren

Eine neue Materie greift § 25a auf. Dies ist eine Reaktion auf Überlegungen, für die polizeiliche Aufgabenerfüllung auch neue Systeme zur Datenanalyse einzusetzen. Der Einsatz solcher Systeme durch die Polizei ist geeignet, 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. Deshalb hat die Konferenz

der Datenschutzbeauftragten des Bundes und der Länder schon in ihrer 89. Konferenz im März 2015 in einer Entschließung darauf hingewiesen, dass die vorhandenen gesetzlichen Vorschriften in Bund und Ländern keine ausdrücklichen Vorgaben für den Einsatz weitgefasster Analysesysteme enthalten (vgl. 44. Tätigkeitsbericht, Ziff. 7.9).

Die Verknüpfung von Daten aus unterschiedlichen polizeilichen Datenbanken sowie ggf. auch die Erweiterung um allgemein zugängliche Daten aus dem Internet stellen Eingriffe in das Recht auf informationeller Selbstbestimmung mit erheblicher Eingriffstiefe dar. Ein solcher ist jedoch nur zulässig, soweit es eine normenklare Rechtsgrundlage gibt.

§ 25a HSOG

(1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

(2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Datenschutzbeauftragte ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

Mit der Definition der möglichen Einsatzbereiche auf die vorbeugende Bekämpfung besonders schwerer Straftaten sowie der Einschränkung auf die Abwehr von schwerwiegenden Gefahren versucht die Regelung, den Anwendungsbereich einzugrenzen. Dies erscheint mir in Abwägung der Interessen der Betroffenen grundsätzlich verhältnismäßig. Ein zusätzliches Sicherungsmoment ergibt sich aus dem Behördenleitervorbehalt und insbesondere auch meiner Beteiligung im Kontext der Errichtung oder wesentlicher Änderungen der automatisierten Anwendungen.

Die Begleitung bzw. Kontrolle entsprechender Projekte wird zukünftig ein wichtiger Aspekt meiner Tätigkeiten im Bereich der polizeilichen Datenverarbeitung sein.

2.6
Novellierung des Hessischen Verfassungsschutzgesetzes

Im Juni 2018 verabschiedete der Hessische Landtag weitgehende Änderungen der gesetzlichen Regelungen für den Verfassungsschutz. Neben organisatorischen Fragen betreffen diese auch grundsätzliche Aspekte im Kontext des informationellen Selbstbestimmungsrechts.

Im November 2017 wurde im Rahmen eines Gesetzentwurfs der Regierungsfraktionen (LTDrucks. 19/5412) die lange angekündigte Reform des Hessischen Verfassungsschutzgesetzes (HVSG) in den Landtag eingebracht und dann im Dezember im Rahmen eines Änderungsantrages (LTDrucks. 19/5782) erweitert.

Eine wesentliche Änderung betrifft die Neugestaltung der Befugnisse des Verfassungsschutzes zur Informationserhebung. Eine erhebliche Auswirkung auf die Rechte der Bürgerinnen und Bürger hat die auch Umgestaltung der Auskunftsregelung. Gleichzeitig wurde die parlamentarische Kontrolle teilweise neu strukturiert und in einem eigenständigen Gesetz geregelt, das jedoch erst mit Beginn der neuen Legislaturperiode im Januar 2019 in Kraft tritt.

Vor der Einbringung der Regelungen im Landtag hatte ich keine Gelegenheit, mich zu den geplanten Änderungen zu äußern. Erst im Rahmen der Anhörung im Landtag konnte ich dazu Stellung nehmen, inwieweit für die vorgesehenen Regelungen und die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung die verfassungsrechtlichen Anforderungen beachtet wurden. Dazu gehört zum einen, dass die Regelungen entsprechend der Rechtsprechung des Bundesverfassungsgerichts normenklar sein müssen sowie dass die wesentlichen Entscheidungen durch den Gesetzgeber selbst zu treffen sind. Diese Anforderungen müssen besonders dann beachtet werden, wenn Detailregelungen nur durch Dienstvorschriften zu treffen sind, auch soweit diese nicht vom Landesamt, sondern vom zuständigen Ministerium erlassen werden sollen.

Ein besonderes Augenmerk meiner Stellungnahme lag daher auf den Regelungen, die der Sicherung der Rechte der Betroffenen dienen. Das gilt vor allem für die Möglichkeiten der Überprüfung des Umgangs mit personenbezogenen Daten sowie insbesondere dem Auskunftsrecht der Bürgerinnen und Bürger. Hier sind nach meiner Einschätzung Einschränkungen der informationellen Selbstbestimmung erfolgt, die dem Grundrechtsschutz nicht gerecht werden. Klare Regelungen sind auch deshalb notwendig, weil die allgemeinen Datenschutzregelungen für öffentliche Stellen für den Verfassungsschutz nicht bzw. nur sehr eingeschränkt gelten.

Die Anhörung im Landtag hat an einigen Punkten der Novelle erhebliche Kritik deutlich werden lassen. Dies galt insbesondere den geplanten neuen Befugnissen wie der Online-Telekommunikationsüberwachung (Quellen-TKÜ) und der Onlinedurchsuchung sowie der Einbeziehung des Verfassungsschutzes in Zuverlässigkeitsüberprüfungen. Im Rahmen eines weiteren Änderungsantrages (LTDrucks. 19/6502) wurde dann von diesen neuen Befugnissen im HVSG abgesehen, diese aber in das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) aufgenommen. Weiter erfolgte eine Anpassung an die zwischenzeitlich erfolgte Neuregelung des Datenschutzrechts im Kontext der europäischen Datenschutzreform und der Verabschiedung des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG).

Kritikpunkte an der neuen gesetzlichen Regelung

Dazu greife ich einige wenige Punkte heraus, für die meines Erachtens weiterhin Nachbesserungsbedarf besteht.

Ausgestaltung der Datenerhebung

Im Gegensatz zur Altregelung sind die Möglichkeiten zur Datenerhebung mit nachrichtendienstlichen Mitteln nunmehr im Gesetz normiert und nicht mehr einer Dienstvorschrift des Innenministeriums überlassen. Die Regelungen für den weiteren Umgang mit diesen Daten sollen sich dann jedoch weiterhin nur aus einer Dienstvorschrift ergeben. Der „Umgang“ mit den erhobenen Informationen ist kein datenschutzrechtlicher Begriff und öffnet daher einen breiten Interpretationsspielraum. Alles Wesentliche zum Eingriff in das Recht auf informationelle Selbstbestimmung hat der Gesetzgeber jedoch selbst zu regeln. Durch diese Formulierung bleibt unklar, welche Regelungsbereiche einer solchen Dienstvorschrift überlassen bleiben, aber auch inwieweit weitere gesetzliche Vorgaben zum Umgang mit den Daten durch eine solche Dienstvorschrift zu beachten oder gar modifizierbar sind.

Auskunft der Betroffenen

Die Voraussetzungen bzw. das Verfahren zur Einholung von Auskünften über Speicherungen durch den Verfassungsschutz wurden erheblich erschwert, wenn nicht gar in der praktischen Anwendung entscheidend beschränkt. Das Auskunftsrecht ist wesentliche Grundlage für die Betroffenen, ihre Grundrechte wahrzunehmen und sie damit in die Lage zu versetzen, sich ggf. gegen unberechtigte Datenspeicherungen oder Übermittlungen zur Wehr zu setzen.

§ 26 HVSG

(1) Das Landesamt erteilt der betroffenen Person über zu ihrer oder seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit die betroffene Person hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Legt die betroffene Person nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt nach pflichtgemäßem Ermessen. Die Auskunft erstreckt sich nicht auf

1. *die Herkunft der Daten und die Empfänger von Übermittlungen und*
2. *Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, die betroffene Person macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem von der betroffenen Person dargelegten Auskunftsinteresse.*

Das Landesamt bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Die Auskunftserteilung unterbleibt, soweit durch sie

1. *eine Gefährdung der Erfüllung der Aufgaben zu besorgen ist,*
2. *Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts zu befürchten ist,*
3. *die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes ein Nachteil bereitet würde oder*
4. *Daten oder die Tatsache ihrer Speicherung preisgegeben werden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.*

Die Entscheidung trifft die Behördenleitung oder eine von ihr besonders beauftragte Mitarbeiterin oder ein von ihr besonders beauftragter Mitarbeiter.

(3) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. Sie enthält einen Hinweis auf die Rechtsgrundlage für das Fehlen der Begründung und darauf, dass sich die betroffene Person an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen der oder des Hessischen Datenschutzbeauftragten an die betroffene Person dürfen ohne Zustimmung des Landesamts keine Rückschlüsse auf den Kenntnisstand des Landesamts zulassen.

Gem. § 26 Abs. 1 HVSG ist es notwendig, dass der Betroffene sowohl auf einen konkreten Sachverhalt hinweist als auch ein besonderes Auskunftsinteresse darlegt. Bis zur Neureglung gab es vergleichbare Einschränkungen nicht. Als Begründung wurde im Wesentlichen die Verhinderung eines unverhältnismäßigen Verwaltungsaufwandes angeführt sowie auf die bestehenden Regelungen im Bundesrecht verwiesen. Bei der Wahrung des Grundrechtsschutzes kann der Aufwand jedoch nur eine untergeordnete Rolle spielen. Auch der Verweis auf die Regelung des BVerfSchG überzeugt als Begründung nicht. Für diese Fragestellung ist es gerade nicht erforderlich, dass die gesetzlichen Regelungen bundesweit identisch sind. Wenn überhaupt, kann dies nur einen Einfluss hinsichtlich der Frage haben, in welchem Umfang bzw. in welchen Fällen eine Auskunftserteilung beschränkt oder abgelehnt

werden kann. Die Möglichkeiten zur Einschränkung der Auskunft bzw. der Verweigerung – wie sie jetzt im Gesetz enthalten sind – gab es auch schon in der alten Regelung.

Das Darlegen des besonderen Auskunftsinteresses soll auch dazu dienen, Ausforschungsversuche zu verhindern. Ich habe Zweifel, ob dies ein geeignetes Mittel dafür ist. Wer wirklich zur Ausforschung sein Auskunftsrecht missbrauchen will, wird in der Lage sein, sein Interesse entsprechend zu formulieren. Andererseits wird jeder andere gezwungen zu begründen, warum er ein Grundrecht wahrnehmen will. Soweit es Anhaltspunkte für ein solches Vorgehen gibt, war auch bisher schon die Verweigerung der Auskunft zulässig.

Mir ist nicht bekannt geworden, dass unter der alten Rechtslage das Auskunftsrecht im großen Umfang zu Ausforschungszwecken missbraucht worden ist.

Mitwirkung an Zuverlässigkeitsüberprüfungen

Neu geschaffen wurde die ausdrückliche Befugnis, Erkenntnisse des Verfassungsschutzes in Zuverlässigkeitsüberprüfungen mit einzubeziehen. Im Gesetz selbst wird dies allerdings nicht im Rahmen der Befugnisse, sondern nur im Rahmen der zulässigen Datenübermittlungen in § 20 geregelt.

§ 20 HVSG

(1) Das Landesamt darf Informationen einschließlich personenbezogener Daten, auch wenn sie mit nachrichtendienstlichen Mitteln erhoben wurden, an inländische öffentliche Stellen übermitteln, wenn der Empfänger die Informationen benötigt

1. *zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit oder der Strafverfolgung, soweit die Übermittlung nicht nach Abs. 2 beschränkt ist, oder*
2. *zur Erfüllung anderer ihm zugewiesener Aufgaben, sofern er dabei auch zum Schutz der freiheitlichen demokratischen Grundordnung beizutragen oder Gesichtspunkte der öffentlichen Sicherheit oder auswärtige Belange zu würdigen hat, insbesondere bei*

   …

   c) der Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben, mit deren Einwilligung,

   …

   g) der Überprüfung der Zuverlässigkeit von Personen nach den bewachungs- und gewerberechtlichen Vorschriften, insbesondere

      aa) der Zulassung von Personen für den zugangsgeschützten Sicherheitsbereich von Veranstaltungen,

      bb) von an der Hessischen Erstaufnahmeeinrichtung für Flüchtlinge und ihren Außenstellen beschäftigtem Sicherheitspersonal,

      cc) von an kommunalen Flüchtlingsunterkünften eingesetztem Wachpersonal,

h) der Überprüfung der Zuverlässigkeit von an der Hessischen Erstaufnahmeeinrichtung für Flüchtlinge und ihren Außenstellen beschäftigten Dolmetscherinnen und Dolmetschern,

i) der anlassbezogenen Überprüfung der Zuverlässigkeit von Personen und Organisationen, mit denen die Landesregierung zusammenarbeitet

aa) in begründeten Einzelfällen,

bb) anlässlich der erstmaligen Förderung von Organisationen mit Landesmitteln, sofern diese in Arbeitsbereichen zur Bekämpfung von verfassungsfeindlichen Bestrebungen tätig werden sollen,

mit deren Einwilligung und der Möglichkeit zur Stellungnahme,

…

Die definierten Fälle erscheinen mir allerdings zum Teil sehr weit gefasst. Voraussetzung solcher Überprüfungen auch für die einzelne Person müsste immer sein, dass es Anhaltspunkte dafür gibt, dass es im konkreten Einzelfall erforderlich ist. Eine pauschale Einbeziehung ganzer Organisationen oder Personengruppen ist nicht vereinbar mit dem Verhältnismäßigkeitsprinzip. Zwar wurde auch hier im Rahmen des Gesetzgebungsverfahrens bezogen auf die Förderung von Organisationen mit Landesmitteln bzw. auch der Zusammenarbeit von Personen in Projekten der Landesregierung nachgebessert, aber weiterhin ist der Rahmen noch sehr weit gefasst. Nach meiner Einschätzung werden Organisationen bei der erstmaligen Förderung unter einen Generalverdacht gestellt, ohne dass im Einzelnen Anhaltspunkte für die Erforderlichkeit einer solchen Überprüfung, die mit den konkret zu prüfenden Personen in Zusammenhang stehen, vorliegen müssen.

Auch die Möglichkeit der Überprüfung von Bewerbern für den Öffentlichen Dienst erinnert an die Regelüberprüfung im Rahmen des Radikalenerlasses aus den 70er Jahren des vorigen Jahrhunderts.

Datenschutzrechtliche Kontrolle der Tätigkeit des Landesamtes für Verfassungsschutz

Aufgrund der Neuregelungen im Datenschutzrecht und da der Verfassungsschutz ausdrücklich von der Anwendung der DS-GVO ausgenommen ist gem. Art. 2 Abs. 2 lit. a DS-GVO, ist in § 15 bestimmt, welche Vorschriften des HDSIG zusätzlich zu den Regelungen des HVSG zur Anwendung kommen. Im Gegensatz zur Mehrzahl der Verwaltungen ist durch diese Regelung mein Kompetenzbereich weiterhin sehr eingeschränkt. Denn auch zukünftig kann ich nur Beanstandungen aussprechen. Von den neuen Befugnissen, die ich z. B. gegenüber der Polizei habe, ist mir nur noch eine Warnung möglich, dass eine geplante Datenverarbeitung gegen datenschutzrechtliche Regelungen verstößt. Damit habe ich weiterhin nur begrenzte Möglichkeiten, im Interesse

der Betroffenen darauf hinzuwirken, dass deren Rechte eingehalten werden. Im Kontext der Verschärfung der genannten Anforderungen an die Auskunftserteilung stellt dies aus meiner Sicht eine erhebliche Einschränkung dar, für die eine tragfähige Rechtfertigung im Gesetzgebungsprozess nicht erfolgte.

Parlamentarische Kontrolle des Landesamtes

Die Regelungen zur Parlamentarischen Kontrolle des Verfassungsschutzes finden sich nunmehr in einem eigenständigen Gesetz, dem Verfassungsschutzkontrollgesetz. Die Regelungen unterscheiden sich nur wenig von den derzeitigen Regelungen. Änderungen sollten nach der Begründung sich in weiten Teilen an dem Kontrollgremiumgesetz des Bundes orientieren. Nicht in allen Punkten ist es jedoch gelungen, die neuen und die bestehenden Regelungen sinnvoll miteinander in Einklang zu bringen.

Neu ist unter anderem, dass nunmehr der Parlamentarischen Kontrollkommission (PKK) eine Geschäftsstelle eindeutig zugeordnet wird. Eine Aufgabenzuordnung für diese Geschäftsstelle gibt es allerdings nicht. Die Protokollführung der Sitzungen wird weiterhin der Kanzlei des Landtages übertragen. Es gibt weiterhin keine Vorgabe zum Sitzungsrhythmus; lediglich für die vorzulegenden Berichte werden Fristen genannt. Eine echte Stärkung der parlamentarischen Verantwortung ist dies nicht.

Auch die Regelung, dass die Mitglieder der PKK zwar mit benannten Mitarbeiterinnen und Mitarbeitern Angelegenheiten der Kontrollkommission erörtern dürfen, aber eine Klarstellung fehlt, dass diese dazu auch Unterlagen für die Beratungen einsehen dürfen, erscheint mir nicht gelungen. Eine sinnvolle Beratung kann häufig abstrakt ohne Unterlagen nicht erfolgen. Da es sich oft um Unterlagen handeln wird, die der besonderen Geheimhaltung bedürfen, und zudem auch personenbeziehbare Angaben Gegenstand sein können, wäre eine ausdrückliche Erlaubnis im Gesetz sinnvoll gewesen.

Ob daher diese eher marginalen inhaltlichen Änderungen im Vergleich zur alten Regelung zu einer effektiveren Kontrolle des Verfassungsschutzes durch die PKK führen können, muss die zukünftige Praxis zeigen.

2.7
Vermehrte gesetzliche Prüfpflichten

Verstärkt hat der Gesetzgeber die Datenschutzbeauftragten konkret verpflichtet, regelmäßige Kontrollen einzelner Datenverarbeitungsverfahren durchzuführen. Teilweise wird dabei ausdrücklich ein bestimmter Prüfzyklus

vorgegeben. Dies bindet erhebliche Personalkapazitäten auch zu Lasten der Erfüllung anderer Aufgaben meiner Dienststelle.

Bereits zum gegenwärtigen Zeitpunkt gibt es eine Vielzahl von gesetzlichen Prüfpflichten. Durch Landes-, Bundes- und EU-Gesetze kommen stetig neue hinzu. Erstmals in seiner Entscheidung zum Antiterrordateigesetz (ATDG) im Jahr 2013 hat das Bundesverfassungsgericht (BVerfG) ausdrücklich eine bestimmte Prüffrequenz für die Datenschutzbeauftragten gefordert (1 BvR 1215/07, BVerfGE 133, 277-377). Das Gericht hatte ausgeführt: „Weil eine Transparenz der Datenverarbeitung und die Ermöglichung individuellen Rechtsschutzes durch das Antiterrordateigesetz nur sehr eingeschränkt sichergestellt werden können, kommt der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu. Der Verhältnismäßigkeitsgrundsatz stellt deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen“ (Rdnr. 214). Daraus hat das Gericht dann entsprechende Anforderungen an die Kontrolle durch die Datenschutzbeauftragten formuliert: „Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen“ (Rdnr. 217).

Als Reaktion auf diese Entscheidung wurde dann Ende 2014 in der Novellierung des ATDG die Pflicht zur Prüfung alle zwei Jahre festgeschrieben.

§ 10 ATDG

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 24 Absatz 1 des Bundesdatenschutzgesetzes dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die von den Ländern in die Antiterrordatei eingegebenen Datensätze können auch von den jeweiligen Landesbeauftragten für den Datenschutz im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden, soweit die Länder nach § 8 Absatz 1 verantwortlich sind. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit arbeitet insoweit mit den Landesbeauftragten für den Datenschutz zusammen.

(2) Die in Absatz 1 genannten Stellen sind im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes zu kontrollieren.

Bei dieser Verpflichtung ist es nicht geblieben. Neben weiteren bundesgesetzlichen Regelungen ist nunmehr auch im HSOG eine entsprechende Verpflichtung enthalten. Weitere Verpflichtungen ergeben sich im Kontext von Datenverarbeitungen im Rahmen der Europäischen Union. Die einzelnen Verpflichtungen unterscheiden sich zum Teil in der Frequenz, aber auch in der Anzahl der jeweils zu überprüfenden Stellen. Dabei sind insbesondere

von der EU derzeit noch weitere Verfahren in Planung, die zusätzliche Verpflichtungen schaffen werden.

Ein Überblick über den derzeitigen Stand ergibt sich aus der folgenden Tabelle. Nicht vollständig erfasst sind weitere Verpflichtungen, die aufgrund der Zuständigkeitsverteilung innerhalb der Bundesrepublik zwar dem BfDI obliegen, für die aber eine Unterstützung durch die Landesbeauftragten erfolgen muss, weil nur diese berechtigt sind, die Rechtmäßigkeit der zugrundeliegenden Datenspeicherungen, die durch Landesbehörden in den jeweiligen Dateien erfolgen, zu überprüfen.

Gegenstand der Prüfung	Rechtsgrundlage	zu prüfende Stelle(n)	Prüfturnus
a) Bundesrechtliche Prüfpflichten			
Antiterrordatei (ATD)	§ 10 Abs. 2 ATDG	LKA u. LfV	alle 2 Jahre
Rechtsextremismusdatei (RED)	§ 11 Abs. 2 RED-G	LKA u. LfV	alle 2 Jahre
b) EU-Rechtsinstrumente			
Schengener Informationssystem (SIS II) – Verarbeitung der SIS II-Daten (einschließlich deren Übermittlung und Austausch sowie der Weiterverarbeitung von Zusatzinformationen.	Art. 44 Abs. 1 VO 1987/2006/EG i. V. m. Art. 60 Abs. 1 Beschluss 2007/533/JI-Rat	LKA	Datenverarbeitungsvorgänge im N.SIS II: alle 4 Jahre (Unterstützung für BKA) im Übrigen (v. a. Datenabrufe und -weiterverarbeitung): regelmäßig
Visa-Informationssystem (VIS) – Verarbeitung der VIS-Daten (einschl. der Übermittlung an das und vom VIS)	Art. 41 Abs. 1 VO 767/2008/EG i. V. m. Art. 8 Abs. 5 und 6 Beschluss 2008/633/JI-Rat i. V. m. § 4 VISZG (VIS-Zugangs-gesetz)	LKA und PPs ggf. weitere Behörden	Abfragen der Sicherheitsbehörden nach VIS-Zugangsbeschluss alle 4 Jahre im Übrigen: regelmäßig
European Dactyloscopy-System (Eurodac) – Verarbeitung der Eurodac-Daten (einschl. deren Übermittlung an und von Eurodac)	Art. 32 Abs. 2, 33 Abs. 2 VO 603/2013/EU	alle angeschlossenen Behörden (Polizei; Ausländerämter)	jährlich

c) Landesrechtliche Prüfpflichten			
HSOG	§ 29a	alle Polizeibehörden	mindestens alle 2 Jahre; gemäß § 28 Abs. 2 protokollierte verdeckte Maßnahmen sowie Übermittlungen im Internationalen Bereich

Neben der Kontrolle, ob die einzelnen Daten in den jeweiligen Datenbanken zu Recht gespeichert sind, kommt zum Beispiel auch eine Prüfung daraufhin in Betracht, ob die Verfahren und Bedingungen für die Abfrage eingehalten wurden.

Solche Prüfungen verursachen einen erheblichen Personalaufwand. Eine Kontrolle von Zugriffsrechten umfasst zunächst eine Auswertung vorhandener Protokollierungen. Dafür sind nicht in allen Fällen Tools vorhanden, die eine sinnvolle Auswertung der jeweiligen Protokolldateien erleichtern. So können die im Rahmen der Nutzung der ATD anfallenden Protokolldateien zwar nach vergebenen Parametern ausgewertet werden, Ergebnis ist aber häufig trotzdem eine Darstellung in Form einer pdf-Datei, die mehrere 100 Seiten umfassen kann. Ob die jeweiligen Zugriffe berechtigt waren, kann nur durch eine parallele Einsicht in die zugrundeliegenden Akten/Verwaltungsvorgänge beurteilt werden.

Das hat zur Konsequenz, dass selbst bei einer sehr klein gehaltenen Stichprobe eine solche Überprüfung mit allen Vor-und Nachbereitungen mehrere Tage dauert und jeweils mindestens zwei bis drei Mitarbeiter bindet. Dabei sind die Überprüfungen der technischen Gegebenheiten noch nicht mitberücksichtigt.

Das BVerfG hat in seiner Entscheidung auch ausdrücklich auf die Rahmenbedingungen für eine adäquate Kontrolle durch die Datenschutzbeauftragten hingewiesen: „Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu. Dies ist bei ihrer Ausstattung zu berücksichtigen“ (Rdnr. 217).

Mit dem derzeitigen Personalkörper können alle diese Verpflichtungen nicht angemessen erfüllt werden. Dies ist auch nicht durch eine andere Schwerpunktbildung erreichbar, da auch die Bearbeitung von Beschwerden und die Erfüllung meiner weiteren Aufgaben gemäß der DS-GVO sowie des § 7 HDSIG nicht zugunsten der Pflichtprüfungen vernachlässigt werden dürfen.

3. Datenschutzbericht bis 24.05.2018 (nach HDSG und BDSG)

3.1 Allgemeine Verwaltung, Kommunen, Soziales

3.1.1 Datenübermittlung an Religionsgemeinschaften zur Festsetzung der Ortskirchensteuer

Die Kommunen sind nicht berechtigt, die Daten aller Grundsteuer A-Pflichtigen an das Kirchensteueramt zu übermitteln, damit dieses die Ortskirchensteuer für die evangelischen Gemeindemitglieder festsetzen kann.

Zwei Kommunen haben sich an meine Dienststelle gewandt und gefragt, ob es zulässig sei, die Daten aller Grundsteuer A-Pflichtigen an das evangelische Kirchensteueramt zu übermitteln. Das Kirchensteueramt setzt anhand der Steuerdaten der Kommunen die Ortskirchensteuer für ihre Gemeindemitglieder fest.

Grundsätzlich sind die Finanzbehörden gemäß § 31 Abs. 1 Satz 1 Abgabenordnung (AO) verpflichtet, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts einschließlich der Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermessbeträge oder Steuerbeträge anknüpfen. Allerdings entfällt diese Verpflichtung, wenn die Zusammenstellung der gewünschten Datenbestände einen unverhältnismäßig hohen Aufwand bedeuten würde (§ 31 Abs. 1 Satz 2 AO). Dies kann z. B. dann gegeben sein, wenn die Kommune die gewünschten Informationen gar nicht nach Kirchenmitgliedschaft gesondert zur Verfügung hat.

§ 31 Abs. 1 Satz 1 und 2 AO

Die Finanzbehörden sind verpflichtet, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts einschließlich der Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermessbeträge oder Steuerbeträge anknüpfen. Die Mitteilungspflicht besteht nicht, soweit deren Erfüllung mit einem unverhältnismäßig hohen Aufwand verbunden wäre.

So verhielt es sich bei den anfragenden Kommunen. Beide Kommunen argumentierten, dass sie nicht das nötige Personal hätten, um die Daten der evangelischen Gemeindemitglieder aus den Daten aller Steuerpflichtiger

herauszusortieren. Dies haben sie dem evangelischen Kirchensteueramt mitgeteilt. Das Kirchensteueramt erwiderte hierauf, dass andere Kommunen unter diesen Umständen die Daten aller Grundsteuer A-Pflichtigen dem Kirchensteueramt zur Verfügung gestellt hätten. Dieses habe dann die Auswertung der Datensätze übernommen und die Daten der evangelischen Gemeindemitglieder extrahiert.

Bei dieser Vorgehensweise erhält das Kirchensteueramt also auch Steuerdaten von Steuerpflichtigen anderer Konfessionen und Glaubensrichtungen sowie Konfessionslosen. Für diesen Personenkreis ist das Kirchensteueramt aber nicht berechtigt, Steuern festzusetzen. Mit anderen Worten: Die Daten sind für die Aufgabenerfüllung des Kirchensteueramtes nicht erforderlich und ihre Übermittlung ist in keiner Weise von der oben zitierten Rechtsvorschrift gedeckt.

Ich habe den Kommunen deshalb mitgeteilt, dass ich die Datenübermittlung der Steuerdaten von allen Grundsteuer A-Pflichtigen an das Kirchensteueramt für unzulässig halte. Lediglich die Daten der Steuerpflichtigen, die der evangelischen Kirche angehören, hätten zulässigerweise an das Kirchensteueramt übermittelt werden dürfen.

Eine Rücksprache beim Hessischen Ministerium der Finanzen hat mich in dieser Auffassung bestätigt. Das Ministerium verwies ergänzend auf § 8 des Kirchensteuergesetzes, wonach die Landes- und Gemeindebehörden den Kirchen (Kirchengemeinden) auf Anforderung die für die Besteuerung **erforderlichen** Daten übermitteln, soweit diese von den Behörden bereits zu anderen Zwecken erhoben werden und soweit die Verwaltung der Kirchensteuern nicht den Finanzämtern obliegt.

3.1.2
Amtshilfe der Sozialverwaltung auf Ersuchen eines Finanzamtes

Die Übermittlung personenbezogener Daten durch eine Sozialbehörde an das Finanzamt kann nicht auf das Amtshilfeprinzip gestützt werden, sondern benötigt eine datenschutzrechtliche Befugnisnorm.

Ein Jobcenter bat mich um datenschutzrechtliche Beurteilung im Hinblick auf ein Auskunftsersuchen eines Finanzamtes. Konkret ging es um personenbezogene Daten eines Leistungsempfängers des Jobcenters. Gestützt wurde das Ersuchen seitens des Finanzamtes auf § 111 Abs. 1 AO sowie § 3 SGB X.

Der vom Finanzamt genannte § 3 SGB X betrifft die „Amtshilfe“ genannte Kooperation von Behörden.

§ 3 Abs. 1 SGB X

Jede Behörde leistet anderen Behörden auf Ersuchen ergänzende Hilfe (Amtshilfe).

Diese im Ersten Kapitel des Zehnten Buches des SGB platzierte Vorschrift wird allerdings durch das im Zweiten Kapitel des Zehnten Buches geregelte Sozialdatenschutzrecht verdrängt, soweit es bei der Ermittlung des Sachverhaltes um personenbezogene Daten (Sozialdaten) geht. Dies ergibt sich aus § 37 S. 3 SGB I.

§ 37 Satz 3 SGB I

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

Dies hat zur Konsequenz, dass insoweit das Sozialdatenschutzrecht vorrangig in den Blick genommen werden muss. In Bezug auf den konkreten Kontext, also das Ersuchen des Finanzamtes (und die Sicherung des Steueraufkommens), gibt es denn auch eine Vorschrift, die diese Thematik zum Gegenstand hat (§ 71 Abs. 1 Nr. 3 SGB X).

§ 71 Abs. 1 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten

…

3. zur Sicherung des Steueraufkommens nach ... § 111 Abs. 1 der Abgabenordnung ..., soweit diese Vorschriften unmittelbar anwendbar sind, …

§ 111 Abs. 1 AO legt fest, dass alle Behörden die zur Durchführung der Besteuerung erforderliche Amtshilfe zu leisten haben.

Diese Vorschrift ist auch im vorliegenden Fall, also dem Ersuchen eines Finanzamtes, unmittelbar anwendbar, so wie von § 71 Abs. 1 Nr. 3 SGB X gefordert. Unmittelbare Anwendbarkeit im Sinne dieser Vorschrift ist nur dann nicht gegeben, wenn nicht die Finanzverwaltung des Landes, sondern Kommunen Steuern erheben (vgl. etwa Rombach in Hauck/Noftz, SGB X, § 71 Rdnr. 6, 35).

Dementsprechend habe ich dem Jobcenter mitgeteilt, dass es zwar nicht mit Blick auf die Begründung des Finanzamtes, dennoch aber im Ergebnis datenschutzrechtlich zulässig ist, dem Ersuchen des Finanzamtes nachzukommen.

3.1.3
Nutzung von Freitextfeldern bei e-meld21 ist unzulässig

Die Nutzung von Freitextfeldern bei e-meld21 ist unzulässig; vorhandene Inhalte sind zu löschen.

Das von der ekom21 angebotene und bei hessischen Einwohnermeldeämtern genutzte Datenverarbeitungsprogramm e-meld21 verfügt über ein Freitextfeld, welches gemeinhin als „Sachbearbeiterinformation“ bezeichnet wird. Dass ein solches Feld bei der Bearbeitung zweifelsfrei hilfreich sein kann, um beispielsweise Bearbeitungsstände oder andere bearbeitungsrelevante Hinweise zu hinterlegen, die damit auch anderen Nutzern zur Kenntnis gelangen, erscheint nachvollziehbar.

Problematisch ist diese Ausgestaltung jedoch vor dem Hintergrund der rechtlichen Bestimmungen im Bundesmeldegesetz und dem Umstand, dass das Freitextfeld, mit oder ohne Inhalte, Teil des melderechtlichen Datensatzes gemäß § 3 BMG ist. Dort sind die möglichen und rechtlich zulässigen Inhalte katalogmäßig und abschließend aufgezählt. Hieraus ergibt sich, dass hier keine weiteren Daten gespeichert werden dürfen, wozu jedoch ein Freitextfeld eine tatsächliche Möglichkeit eröffnet. Die Nutzung des Freitextfeldes ist daher abschließend als unzulässig zu betrachten.

Soweit ein Freitextfeld im melderechtlichen Datensatz tatsächlich noch Inhalte aufweist, erstreckt sich natürlich auch das Auskunftsrecht gemäß § 10 BMG auf diese Inhalte, d. h., was dort vermerkt ist, ist vorbehaltlos an den Betroffenen zu beauskunften.

3.1.4
Videoüberwachung in Schwalbach am Taunus

Nicht die Zahl der Kameras entscheidet über die Zulässigkeit einer Videoüberwachungsanlage gemäß § 14 Abs. 3 HSOG.

Seit Sommer 2017 wurde die Errichtung einer Videoüberwachungsanlage in Schwalbach am Taunus (Bereich Marktplatz/Zentrum) durch mich beratend begleitet.

Die Videoüberwachung sollte eingesetzt werden, da im genannten Bereich immer wieder ein erhöhtes Kriminalitätsaufkommen zu verzeichnen war. Neben Beschädigungen an Gewerbeobjekten kam es auch zu einem Brandanschlag auf eine Pizzeria und Angriffen auf Polizeibeamte. Die Kriminalitätsentwicklung konnte anhand polizeilich erhobener Daten aus der

polizeilichen Kriminalstatistik nachvollzogen werden und ließ den Bereich qualitativ und quantitativ als Kriminalitätsschwerpunkt erscheinen.

Zunächst wurde dort temporär eine polizeiliche Videoüberwachungsanlage auf dem Dach des Rathauses installiert. Nach dem Willen des Magistrats der Stadt Schwalbach am Taunus und des zuständigen Polizeipräsidiums Westhessen sollte die temporäre Anlage der Polizei durch eine fest installierte Anlage ersetzt werden. Diese sollte nun nicht mehr alleine von der Polizei, sondern auch von dem Ordnungsamt als Gefahrenabwehrbehörde der Stadt Schwalbach am Taunus betrieben werden. Dies war möglich, da die rechtlichen Voraussetzungen gemäß § 14 Abs. 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) für beide Behörden identisch sind.

§ 14 Abs. 3 HSOG

Die Gefahrenabwehr- und 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 sowie der Name und die Kontaktdaten der oder des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen. Abs. 1 Satz 2 und 3 gilt entsprechend.

Kritisch gesehen wurde die Ausgestaltung der Überwachungsanlage. In diesem Zusammenhang fand mit meiner Beteiligung im April 2018 eine Informationsveranstaltung im Rathaus Schwalbach am Taunus statt, bei der interessierte Bürgerinnen und Bürger auch Fragen zu datenschutzrechtlichen Aspekten der Videoüberwachungsanlage stellen konnten.

Dabei konnte insbesondere geklärt werden, dass allein die recht hoch anmutende Zahl von 17 Kameras nicht zur Unzulässigkeit der Videoüberwachung führte. Die Anzahl der eingesetzten Kameras ist an sich nicht von rechtlicher Relevanz und stellt auch keinen Parameter für eine Eingriffstiefe dar. Entscheidend ist vielmehr die Erforderlichkeit der einzelnen Kameras im Hinblick auf den Zweck, einen Kriminalitätsschwerpunkt zu entschärfen.

Im vorliegenden Fall war die Anzahl der Kameras der besonderen Bebauung des überwachten Bereichs geschuldet. Es galt zu vermeiden, dass aufgrund der etwas unübersichtlichen Gebäudekonstellation nicht einsehbare Bereiche entstehen. Auch Betrieb und Zugriffsberechtigungen konnten geklärt werden. Die nun fest installierte Anlage wird von der Polizei und dem Ordnungsamt der Stadt betrieben. Beide Behörden haben Zugriff auf die Videosequenzen.

Vor der endgültigen Inbetriebnahme habe ich sämtliche Kameraeinstellungen überprüft und – soweit erforderlich – Anpassungen herbeigeführt. Durch

Einsatz entsprechender Verpixelungstechniken konnte ich erreichen, dass Kameras auch bei Schwenkungen und Fokussierungen keine Daten aus sog. Privatschutzzonen erheben. Ein Hineinspähen in Privatwohnungen, auf Balkone, in Gastronomiebereiche und Ladenlokale wird damit technisch verhindert. Die erhobenen Daten (Videoaufnahmen) dürfen für zehn Tage gespeichert werden und können, falls erforderlich, als Beweismittel in Ermittlungsverfahren herangezogen werden.

3.2
Schulen, Hochschulen

3.2.1
Ohne Führungszeugnis und Gesundheitsauskunft zum Schulbesuch

Die Forderung nach Vorlage eines polizeilichen Führungszeugnisses und/oder Auskünften zum Gesundheitszustand eines Bewerbers ist im Rahmen des Aufnahmeverfahrens einer Schule datenschutzrechtlich unzulässig.

Durch den Hinweis eines Betroffenen bin ich darauf aufmerksam geworden, dass staatliche Schulen der Erwachsenenbildung im Rahmen des Aufnahmeverfahrens von Schülerinnen und Schülern ein polizeiliches Führungszeugnis anfordern. Ein Schüler hatte ein Aufnahmeverfahren durchlaufen und sollte als Unterlagen u. a. ein polizeiliches Führungszeugnis vorlegen. Auch wurden in dem Aufnahmebogen Fragen zum gesundheitlichen Zustand des angehenden Schülers gestellt. Der Betroffene erachtete das Verfahren als unverhältnismäßig und dem Zweck nicht angemessen.

Die betroffenen Schulleitungen leiteten die Rechtmäßigkeit ihres Handelns aus einem Erlass als Anlage der Verordnung zur Ausgestaltung der Schulen für Erwachsene (SfEAusgV) ab. Darin heißt es:

„*Einer Bewerbung um Aufnahme an eine Schule für Erwachsene sind folgende Unterlagen beizufügen: 1. Geburtsurkunde, ersatzweise eine Kopie der Personaldokumente; ein polizeiliches Führungszeugnis kann verlangt werden; 2. […]*“.

Die Vorgabe in dem bezeichneten Erlass halte ich für datenschutzrechtlich unzulässig, weil nicht erforderlich. Ich habe mich deshalb schriftlich unmittelbar an den Erlassgeber, das Hessische Kultusministerium (HKM), gewandt.

In meinem Schreiben habe ich festgestellt, dass weder das Hessische Schulgesetz noch die Verordnung zur Verarbeitung personenbezogener Daten an Schulen eine Norm enthalten, die im Zusammenhang mit einem Aufnahmeverfahren für eine wie auch immer geartete Schulform die Vorlage einer Auskunft aus dem Bundeszentralregister erfordert oder vorsieht.

Vielmehr sind die Schulen nur berechtigt, jene Daten von Schülern und Eltern sowie den Lehrkräften zu erheben, die zur rechtmäßigen Erfüllung des Erziehungs- und Bildungsauftrages der Schule und den jeweils damit verbundenen Zweck, zur Durchführung schulorganisatorischer Maßnahmen oder zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich sind (§ 83 Abs. 1 HSchG und § 1 Abs. 1 der Verordnung zur Verarbeitung personenbezogener Daten in Schulen). Dazu zählt die Vorlage eines Führungszeugnisses nicht.

§ 83 Abs. 1 HSchG

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrern verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist.

§ 11 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist … zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der datenverarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

Auch im Sinne des § 11 Abs. 1 HDSG war die Anforderung eines polizeilichen Führungszeugnisses unzulässig. Die Datenverarbeitung muss für den jeweiligen Zweck erforderlich sein. Ein Erfordernis für die Erhebung von Daten aus einem Register, insbesondere einem polizeilichen Führungszeugnis, habe ich nicht erkennen können. Selbst im Rahmen des Beschäftigungsverhältnisses von Arbeitnehmern ist die Forderung des Arbeitgebers nach einem Führungszeugnis restriktiv auszulegen. So hat das Bundesarbeitsgericht in einem Urteil vom 17.11.2016 zu diesem Thema ausgeführt:

„Der mit der Datenerhebung verbundene Eingriff in das allgemeine Persönlichkeitsrecht des Arbeitnehmers muss auch im Rahmen von § 32 Abs. 1 Bundesdatenschutzgesetz einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten.“

In meinem Schreiben hatte ich zudem darauf bestanden, dass das Ministerium veranlasst, bereits vereinnahmte und in der Regel in der Schülerakte abgelegte Führungszeugnisse daraus zu entfernen und die Dokumente den Betroffenen zurückzugeben oder, soweit dies nicht möglich ist, zu vernichten.

Schließlich hatte ich das Kultusministerium auch darauf aufmerksam gemacht, dass die Erhebung von Gesundheitsdaten im Zusammenhang mit dem Aufnahmeverfahren ebenfalls einer Rechtsgrundlage entbehrt.

Das Kultusministerium teilt meine Rechtsauffassung uneingeschränkt

Das Hessische Kultusministerium hat meine Rechtsposition in allen kritisierten Punkten geteilt und mir mitgeteilt, Maßnahmen zur Abhilfe eingeleitet zu haben. So wurde im Erlassweg allen Schulen die Anwendung der in Rede stehenden „Kann-Formulierung“ in Bezug auf die Vorlage von polizeilichen Führungszeugnissen untersagt. Im gleichen Zusammenhang wurde eine Novellierung der Verordnung zur Ausgestaltung der Schulen für Erwachsene (SfEAusgV) angekündigt. Bis zu deren Rechtsetzung schließt der Erlass eine Anwendung der „Kann-Formulierung“ aus.

Zusätzlich hat das Ministerium in einer Sitzung der Schulen für Erwachsenenbildung den Schulleitungen die künftige Verfahrensweise mündlich erläutert. Die Schulen wurden angewiesen, sämtliche Hinweise und Verlautbarungen in Bezug auf die Vorlage von polizeilichen Führungszeugnissen von den Veröffentlichungen, Werbematerialien und/oder sonstigen Medien der Schule und von sämtlichen Aufnahmedokumenten zu entfernen. Außerdem wurde veranlasst, alle Schülerakten auf bereits vorgelegte Führungszeugnisse zu durchforsten und diese den Betroffenen zurückzugeben, soweit dies möglich ist. Im anderen Fall besteht die Verpflichtung, das Dokument zu löschen oder zu vernichten.

Auch hinsichtlich der Erhebung von Gesundheitsdaten schloss man sich meiner Auffassung an. Das Hessische Kultusministerium hat gegenüber den Schulleitungen ebenfalls klargestellt, dass die Erhebung von Gesundheitsdaten oder Fragen nach dem Gesundheitszustand im Zuge von Aufnahmeverfahren unzulässig sind. Entsprechende Unterlagen, soweit diese in Schülerakten vorhanden sind, sind ebenfalls daraus zu entfernen und zu vernichten.

3.2.2
Datenschutzkonforme Gestaltung der Ausschreibungsverfahren zur Beförderung gesundheitlich beeinträchtigter Schüler/-innen in Hessen

Die bisherige Gestaltung der Ausschreibungsverfahren wird in Hessen nicht einheitlich praktiziert und widerspricht teilweise datenschutzrechtlichen Grundsätzen. Sie ist daher entsprechend anzupassen.

Ein Petent erhob bei meiner Behörde Beschwerde über die Veröffentlichung von 98 Schüler/-innen-Adressdaten im Rahmen eines Ausschreibungsverfahrens zur Schüler/-innenbeförderung. Er trug unter anderem vor, die Adressdaten seien personenbeziehbar und damit einzelnen Schülern/-innen zuzuordnen.

Dieser Beschwerde lag folgender Sachverhalt zugrunde:

Im Februar 2018 veröffentlichte ein Schulamt in Hessen im Rahmen eines offenen Verfahrens auf der Hessischen Ausschreibungsdatenbank eine Ausschreibung zur Schülerbeförderung von schulwegunfähigen Kindern aus der betreffenden Stadt und Vororten zu einer Schule innerhalb dieser Stadt.

Die Hessische Ausschreibungsdatenbank (HAD) beschreibt sich auf ihrer Homepage wie folgt:

„Die Hessische Ausschreibungsdatenbank (HAD) ist eine internetgestützte, allgemein verfügbare Datenbank zur Veröffentlichung von Bekanntmachungen im Rahmen öffentlicher Beschaffungsverfahren. Sie wird im Interesse der gewerblichen Wirtschaft, des Handwerks und Freischaffender in Hessen betrieben, um Beschaffungsvorgänge der öffentlichen Hand mit mehr Wettbewerb, Transparenz und Effizienz auszustatten.

Durch die enge Zusammenarbeit zwischen Ministerien, Wirtschaft und Beschaffungsstellen wird die HAD ständig praxisnah weiterentwickelt. Die HAD ist nicht nur Bekanntmachungsplattform, sondern kostenloser Ansprechpartner für alle technischen, inhaltlichen und rechtlichen Fragen zum Vergabeverfahren.

Die HAD wurde Ende der 90er Jahre von der Auftragsberatungsstelle Hessen e. V. (ABSt) aus einer Beteiligung an dem EG-Projekt ‚Simap-Vergabeplattform' entwickelt. Das EG-Projekt wurde nach Einstellung durch die Europäische Kommission von der ABSt Hessen e. V. als Projekt für das Land Hessen weitergeführt. Seit 2007 ist die HAD eine kostenlose Serviceleistung für alle hessischen Vergabestellen und Unternehmen in Europa. Da per Hessischem Vergabe- und Tariftreuegesetz die Pflicht zur Veröffentlichung aller nationalen und EU-weiten Bekanntmachungen auf der HAD besteht, sind alle hessischen Bekanntmachungen vollständig auf der HAD zu finden. Weiterhin werden wichtige Vergaberegelungen, sei es Richtlinien, Gesetze oder Erlasse und sonstige Rundschreiben zum Vergaberecht insbesondere für die hessische Verwaltung tagesaktuell auf der HAD veröffentlicht."

Dementsprechend wurden im Rahmen dieser Ausschreibung neben dem Namen der Schule einschließlich der jeweils besuchten Schulklassen der betroffenen Schülerinnen und Schüler auch deren Wohnanschriften veröffentlicht (Ortsteil, Straße, Hausnummer). Auch war den Ausschreibungsunterlagen die Tatsache zu entnehmen, dass es sich um gesundheitlich beeinträchtigte Kinder handelte (Schulwegunfähigkeit).

Zwar waren die Namen der Kinder der veröffentlichten Adressliste nicht zu entnehmen, gleichwohl waren zumindest zwei der 98 veröffentlichten Adressdaten im Hinblick auf die Nachnamen der betroffenen Kinder tat-

sächlich personenbeziehbar. Dies ergab eine – anhand dieser Adressliste durchgeführte – umfangreiche Recherche. Nachdem diese beiden Namen jeweils einem Objekt (Einfamilienhaus) zugeordnet werden konnten und damit offenkundig geworden war, dass die grundsätzliche Möglichkeit der Herstellung eines Personenbezuges bestand, war der Sachverhalt eindeutig.

Aufgrund der gesetzlichen Änderungen des Vergaberechts zu öffentlichen Aufträgen müssen die Dokumente zu den Ausschreibungen sowohl national als auch europaweit im Rahmen der Veröffentlichung jedermann ohne technische Beschränkung zugänglich gemacht werden („Barrierefreiheit"). Etwaige Zugangsbeschränkungen zu den Ausschreibungen wurden aufgehoben. Ein von vornherein ausgewählter Adressatenkreis, wie z. B. im vorliegenden Fall Beförderungsunternehmen, existiert nicht (mehr).

Somit war die Kenntnisnahme folgender personenbezogenen Daten auch für – am Ausschreibungsverfahren unbeteiligte – Dritte möglich: Anschriften der betroffenen Kinder, Vorliegen einer gesundheitlichen Beeinträchtigung bei diesen Kindern sowie der Name der besuchten Schule einschließlich der Schulklasse des jeweiligen Kindes.

Durch den barrierefreien Zugang zu diesen Daten werden nunmehr auch Unternehmen, die kein Beförderungsgewerbe betreiben, in die Lage versetzt, die Daten für Ihre Zwecke zu verarbeiten. Denkbar wäre hier beispielsweise das Offerieren von Produktangeboten durch Sanitätshäuser oder Anderen gegenüber den Eltern der betroffenen Kinder, etwa durch Einwerfen von Werbebroschüren in die Briefkästen der Elternhäuser.

Zum Zeitpunkt der Ausschreibung/Veröffentlichung galt noch das Hessische Datenschutzgesetz (HDSG). Seit dem 25.05.2018 ist der Sachverhalt nach der DS-GVO zu beurteilen.

Sowohl nach altem Recht (§ 7 Abs. 4 HDSG) als auch nach neuem Recht (Art. 9 Abs. 1 DS-GVO) unterliegen Gesundheitsdaten einem besonderen Schutz.

§ 7 Abs. 4 HDSG

Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33 bis 35 und 39 erfolgen. Im Übrigen ist eine Verarbeitung auf Grund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist.

Art. 9 Abs. 1 DS-GVO

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Unter den Begriff „Gesundheitsdaten“ sind nicht nur konkrete medizinische Diagnosen zu subsumieren, sondern vielmehr bereits die Tatsache, dass bei einer Person eine gesundheitliche Beeinträchtigung vorliegt, in diesem Falle die Schulwegunfähigkeit der betroffenen Kinder.

Durch die Herstellbarkeit des Personenbezugs war diese Form der Ausschreibung aus datenschutzrechtlicher Sicht unzulässig, sofern es die uneingeschränkte Veröffentlichung

1. sowohl der vollständigen Adressdaten der betroffenen Kinder als auch
2. der Tatsache, dass es sich vorliegend um gesundheitlich beeinträchtigte Kinder handelt,

betraf.

Dies habe ich dem Schulträger auch so mitgeteilt. Daraufhin teilte mir dieser mit, künftig wie folgt zu verfahren:

Für Ausschreibungen der Beförderungsaufträge sei ab dem Schuljahr 2019/2020 ein zweistufiges Ausschreibungsverfahren nach § 41 der Vergaberichtlinie avisiert. Im ersten Schritt werde eine Liste als Anlage zum Leistungsverzeichnis veröffentlicht, die ausschließlich die Straßennamen (ohne Hausnummern) und die Anzahl der voraussichtlich zu befördernden Schülerinnen und Schüler enthalte. Dies diene der Orientierung der Interessenten der Ausschreibung. Nach Vorlage einer Vertraulichkeitserklärung erfolge dann im zweiten Schritt zur Kalkulationsgrundlage die Veröffentlichung der Adresslisten unter Angabe der Hausnummern gesondert an die jeweiligen Interessenten der Ausschreibung.

Dieses Verfahren halte ich für akzeptabel, sofern die Notwendigkeit besteht, die Schülerinnen und Schüler aufgrund ihrer jeweiligen gesundheitlichen Beeinträchtigung unmittelbar an ihrer Wohnanschrift abholen zu müssen.

3.3
Verkehr, Daseinsvorsorge

3.3.1
Übermittlung von Verbrauchswerten durch den Netzversorger bzw. Netzbetreiber an den Vermieter

Der Vermieter hat keinen Herausgabeanspruch gegenüber dem Gasnetzbetreiber bezüglich der Gasverbrauchswerte im vermieteten Versorgungsobjekt.

Mich erreichte in diesem Jahr eine Beschwerde eines Vermieters, der bei dem für das Gebiet des vermieteten Objekts zuständigen Gasnetzbetreiber datenschutzrechtliche Auskunft über die Verbrauchswerte des Gaszählers über mehrere Jahre begehrte. Der Vermieter war Eigentümer eines vermieteten Objekts. Die Abrechnung des Gasverbrauchs erfolgte nicht über den Vermieter, sondern wurde seitens des Gasversorgers direkt mit dem Mieter abgewickelt. Der Gasnetzbetreiber verweigerte aus datenschutzrechtlichen Gründen die Herausgabe, sofern keine Einwilligung des Mieters für die Übermittlung der Gasverbrauchswerte vorgelegt werden könne.

Der Gasnetzbetreiber ist für den Betrieb des Gasnetzes zuständig, der Gasversorger hingegen für die Lieferung des Gases. Grundsätzlich gilt: Den Gasversorger kann man wechseln, den Netzbetreiber nicht. Der Gasversorger zahlt an den Netzbetreiber eine Gebühr für die Netznutzung und die Zähler. Die jeweiligen Gasversorger übermitteln die einzelnen Gasverbrauchswerte dem Gasnetzbetreiber. Diese werden für die Berechnung der Netznutzungsgebühren, die der Gasversorger an den Gasnetzbetreiber zu entrichten hat, benötigt. Somit liegen dem Gasnetzbetreiber sämtliche Verbrauchswerte für eine Messstelle vor. Dem Grundstückseigentümer/Vermieter ist der für das Gebiet zuständige Gasnetzbetreiber bekannt. Der Gasversorger könnte – je nach vertraglichen Verhältnissen – vom Mieter ohne Mitwirkung des Vermieters ausgesucht werden.

Der datenschutzrechtliche Auskunftsanspruch ist an das Vorliegen der personenbezogenen Daten des Anspruchsverlangenden gebunden. Gemäß § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Verbrauchsdaten können Rückschlüsse auf das Heizverhalten des Bewohners, die Zeiträume seiner An- und Abwesenheit und die Nutzung bestimmter Räume ermöglichen, weshalb sie als personenbezogene Daten anzusehen sind (so auch im Urteil vom 28.10.2014 des LG Dortmund, Az: 9 S 1/14, ZMR 2015, S. 330). Die Verbrauchswerte sind personenbezogene Daten des Gasverbrauchers und somit des Mieters. Anspruchsberechtigt

ist daher der Mieter. Der Vermieter kann keine Auskunft aus § 34 BDSG verlangen, weil es sich nicht um seine personenbezogenen Daten handelt.

Jedoch könnte der Vermieter die Verbrauchswerte verlangen, wenn er sein Verlangen auf eine datenschutzrechtliche Grundlage stützen kann. Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist gemäß § 4 Abs. 1 BDSG nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Die Einwilligung des Mieters lag in diesem Fall nicht vor. Eine anderweitige Rechtsgrundlage z. B. im Rahmen eines Mietvertrages (§ 28 Abs. 1 Nr. 1 BDSG) oder aufgrund seines berechtigten Interesses des Vermieters (§ 28 Abs. 1 Nr. 2 BDSG) wurde durch den Vermieter nicht substantiiert vorgetragen.

Daher habe ich das Begehren des Vermieters nicht unterstützt und ihm mitgeteilt, dass er keinen datenschutzrechtlichen Auskunftsanspruch geltend machen kann und sonst kein Erlaubnistatbestand für die Übermittlung der Daten vorgetragen wurde.

3.3.2
Änderung des Verfahrens für die Ausstellung eines sog. Drohnenführerscheins

Für die Erteilung einer Bescheinigung zum Nachweis ausreichender Kenntnisse und Fertigkeiten nach § 21a Abs. 4 Luftverkehrs-Ordnung (sog. Drohnenführerschein) ist es nicht erforderlich, dass die Antragsteller eine Erklärung unterzeichnen, in der sie bestätigen, dass in den letzten fünf Jahren weder ein Ermittlungsverfahren der Staatsanwaltschaft noch ein gerichtliches Strafverfahren, das nicht zu einer Verurteilung geführt hat, gegen sie abgeschlossen wurde.

Ich erhielt einen Hinweis, dass eine zuständige Stelle für die Erteilung von Drohnenführerscheinen von den Antragstellern eine „Erklärung zu Ermittlungsverfahren“ fordert, mit der bestätigt werden muss, dass

– man nicht gerichtlich vorbestraft ist,
– gegen die eigene Person derzeit kein gerichtliches Strafverfahren oder Ermittlungsverfahren der Staatsanwaltschaft anhängig ist und
– gegen einen in den letzten fünf Jahren weder ein Ermittlungsverfahren der Staatsanwaltschaft noch ein gerichtliches Strafverfahren, das nicht zu einer Bestrafung geführt hat, abgeschlossen worden ist.

Seit dem 07.04.2017 gilt in Deutschland die Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten vom 30.03.2017. Sie wurde vom

Bundesministerium für Verkehr und digitale Infrastruktur erlassen und hat die Änderung der Luftverkehrs-Ordnung (LuftVO) und der Luftverkehr-Zulassungs-Ordnung (LuftVZO) zum Gegenstand. Seit diesem Jahr ist es demnach nötig, dass die Betreiber einen Drohnenführerschein besitzen, bevor sie gewisse Arten der Fluggeräte steuern dürfen. Der Drohnenführerschein wird nach Bestehen einer Prüfung ausgestellt. Im Vorfeld der Prüfung sind bestimme Unterlagen vorzulegen. Im Rahmen der Vorlage diese Unterlagen wurde unter anderem auch die gegenständliche Erklärung zu Ermittlungsverfahren verlangt.

Nach datenschutzrechtlichen Vorschriften ist die Erhebung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies vorsieht oder der Betroffene eingewilligt hat. Da die Möglichkeit der Einwilligung den Betroffenen nicht eingeräumt wurde, ist die Erhebung von oben aufgeführten Daten nur dann zulässig, wenn ein Gesetz oder eine Rechtsverordnung die Erhebung zulässt.

Als eine solche Vorschrift wurde von der zuständigen Stelle § 21d Abs. 3 der LuftVO vorgebracht.

§ 21d Abs. 3 LuftVO

Der Bewerber muss das 16. Lebensjahr vollendet haben und hat der anerkannten Stelle vor der Prüfung folgende Unterlagen vorzulegen:

1. *ein gültiges Identitätsdokument,*
2. *bei Minderjährigkeit die Zustimmung des gesetzlichen Vertreters,*
3. *eine Erklärung über laufende Ermittlungs- oder Strafverfahren und*
4. *ein Führungszeugnis nach § 30 Absatz 1 des Bundeszentralregistergesetzes, sofern er sich erstmals um eine Bescheinigung bewirbt.*

Die das Erfordernis des Drohnenführerscheins regelnde Luftverkehrsverordnung ist zwar eine Bundesverordnung und kann somit als datenschutzrechtliche Grundlage fungieren. Jedoch wies ich die zuständige Stelle darauf hin, dass auf § 21d Abs. 3 LuftVO lediglich die Vorlage einer Erklärung über laufende Ermittlungs- oder Strafverfahren sowie eines Führungszeugnisses, in dem die Vorstrafen des Bewerbers enthalten sind, gestützt werden kann. Die Vorlage einer Selbstauskunft, dass gegen den Antragsteller in den letzten fünf Jahren weder ein Ermittlungsverfahren der Staatsanwaltschaft noch ein gerichtliches Strafverfahren, das nicht zu einer Bestrafung geführt hat, abgeschlossen worden ist, wird durch die Norm jedoch nicht angeordnet. Weitere Rechtsgrundlagen konnten nicht genannt werden, sodass ich die Erhebung der Selbstauskunft über abgeschossene Ermittlungs- und Strafverfahren ohne Verurteilung als unzulässig erachtete.

Der für die Ausstellung der Drohnenführerscheine zuständige Stelle änderte daraufhin die Erklärung zu Ermittlungsverfahren entsprechend ab, sodass die Selbstauskunft zu abgeschlossenen Ermittlungs- und Strafverfahren ohne Verurteilung aus der Erklärung zu Ermittlungsverfahren entfernt wurde. Ferner wurden alle Antragsteller, von denen zu Unrecht die Daten erhoben wurden, über die Rechtslage informiert. Alle bereits übermittelten Erklärungen sowie die dazugehörenden Dokumente wurden gelöscht.

3.4
Gesundheitswesen

3.4.1
Akteneinsicht bei der Psychotherapeutenkammer Hessen (LPPKJP Hessen)

Einem Mitglied der LPPKJP Hessen wurde die Akteneinsicht in ein abgeschlossenes Verfahren des Ausschusses für Beschwerde und Schlichtung versagt. Ich habe dies zum Anlass genommen, mich genauer mit den Vorgaben der LPPKJP Hessen in diesem Bereich zu beschäftigen. Im Ergebnis konnte erreicht werden, dass dem betroffenen Mitglied die begehrte Akteneinsicht gewährt wird und dass die Vorgaben der LPPKJP Hessen betreffend die Akteneinsicht überarbeitet werden.

Der Anlass

Ein Mitglied der LPPKJP Hessen schilderte mir, dass eine Beschwerde ihrer Patientin im Jahr 2014 Gegenstand eines Verfahrens im Ausschuss für Beschwerde und Schlichtung der Kammer war. Die Beschwerde wurde schließlich im Jahr 2015 ohne Angabe von Gründen zurückgewiesen. Das Mitglied bat im darauffolgenden Jahr um Akteneinsicht, um Antworten auf ihre offenen Fragen – insbesondere in Hinblick auf die Begründung der Entscheidung – zu erhalten. Diese Bitte wurde von der LPPKJP Hessen unter Berufung auf die Geschäftsordnung des Beschwerdeausschusses der Kammer abgelehnt. Die Geschäftsordnung biete hierfür keine Rechtsgrundlage. Die Akte sei geschlossen und archiviert worden. Da ich die Haltung der Kammer für nicht rechtskonform erachtet habe, bin ich in einen Dialog mit der Kammer getreten. Daraufhin wurde dem Mitglied teilweise Einsicht gewährt. Der von der Kammer als „nicht öffentliches Ergebnisprotokoll“ bezeichnete Teil der Akte, in dem die Gründe für die Entscheidung festgehalten wurden, wurde dem Mitglied jedoch verwehrt. Insbesondere wurde hierfür angeführt, dass dieses Protokoll nicht Bestandteil der Akte sei, da es körperlich getrennt von der Akte in einem verschlossenen Umschlag an die Akte angeheftet werde. Zudem würden solche Protokolle teilweise schützenswerte Daten Dritter

enthalten. Schließlich handele es sich teilweise um Wortlautprotokolle, bei denen auch auf andere ähnlich gelagerte Fälle Bezug genommen werde.

Rechtliche Würdigung

Ich habe die Kammer auf die Vorschriften des § 29 HVwVfG und § 18 Abs. 5 HDSG hingewiesen.

§ 18 Abs. 5 HDSG

Sind personenbezogene Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, dann kann er bei der speichernden Stelle Einsicht in die von ihm bezeichneten Akten verlangen. … Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter … derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. … Im Übrigen kann ihm statt Einsicht Auskunft gewährt werden.

§ 29 Abs. 1 HVwVfG

Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. …

Im Rahmen eines förmlichen Verwaltungsverfahrens hat die Regelung zum Einsichtsrecht des § 29 HVwVfG Vorrang vor dem § 18 HDSG (siehe Dembowski in: Schild/Ronellenfitsch/Arlt/Dembowski/Wellbrock/Müller/Piendl/Topp/Wehrmann: HDSG, § 18, Rdnr. 20, 11/2015). Das heißt, dass bis zum Abschluss des Verfahrens die Beteiligten unter den Voraussetzungen des § 29 HVwVfG ein Einsichtsrecht in die Akten geltend machen können. Nach Abschluss des Verfahrens greift dann das Auskunftsrecht des § 18 HDSG (Dembowski, a. a. O.). Danach sind alle Betroffenen, deren personenbezogene Daten in dem Vorgang verarbeitet wurden, zur Auskunft bzw. Einsicht unter den Voraussetzungen des § 18 HDSG berechtigt.

Da es sich bei den landesgesetzlichen Regelungen um höherrangiges Recht handelt, teilte ich der Kammer mit, dass die sehr engen Satzungsregelungen der Kammer zur Akteneinsicht rechtswidrig und mithin nicht anzuwenden waren.

Aktenbegriff

Auch der Standpunkt der Kammer, das „nicht öffentliche Ergebnisprotokoll“ sei nicht Bestandteil der Akte, war aus meiner Sicht nicht vertretbar.

Die Beschwerdeakte ist eine personenbezogene Akte des Kammermitglieds (§ 49 Abs. 3 Heilberufsgesetz). Der datenschutzrechtliche Begriff der „Akte“ ist in § 2 Abs. 7 HDSG legal definiert:

§ 2 Abs. 7 HDSG

Eine Akte ist jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist.

Der Gesetzgeber geht hier von einem umfassenden Aktenbegriff aus. Das „Ergebnisprotokoll“ gibt den Inhalt und das Ergebnis der Beratung des Ausschusses zu dem in der Akte geführten Fall wieder. Es dient der Beurteilung des Falles und wird zudem für die Fälle etwaiger späterer Beschwerden gegen das Kammermitglied aufbewahrt. Es dient daher dem Zweck der Aufgabenerfüllung des Ausschusses, nämlich dem möglichen Fehlverhalten des Kammermitglieds nachgehen zu können. Sollte dies nicht der Fall sein, müsste das Ergebnisprotokoll vernichtet werden. Die physische Trennung des Ergebnisprotokolls von der Akte (zum Beispiel durch einen Ordner oder einen Hefter) kann aus den o. g. Gründen nicht dazu führen, dass dieses nicht Bestandteil der Akte im datenschutzrechtlichen Sinne wird. Vielmehr würde eine solche Betrachtung die aus dem informationellen Selbstbestimmungsrecht resultierenden Akteneinsichts- und Auskunftsrechte umgehen.

Schutz Daten Dritter

Dem Argument der Kammer, die „Ergebnisprotokolle“ würden teilweise schützenswerte Daten Dritter enthalten, setzte ich entgegen, dass der Gesetzgeber in § 18 Abs. 5 Satz 3 HDSG genau solche Konstellationen berücksichtigt habe:

§ 18 Abs. 5 Stz 3 HDSG

Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter … derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Hier hat stets eine Einzelfallprüfung stattzufinden. Lassen sich einzelne Daten vor der Einsicht abdecken oder einzelne Dokumente für die Einsicht durch das Austauschen mit teilweise geschwärzten Kopien ersetzen, kann der Aufwand nicht als unverhältnismäßig eingestuft werden. Dafür, dass im Fall der „Ergebnisprotokolle“ eine Separierung bzw. Schwärzung nicht in Frage käme, weil dies mit einem unverhältnismäßig hohen Aufwand verbunden wäre, sah ich keine Anhaltspunkte.

Ergebnis

Die LPPKJP Hessen gewährte dem Mitglied auch Akteneinsicht in das „nicht öffentliche Ergebnisprotokoll“. Die Daten unbeteiligter Dritter wurden geschwärzt.

In die geänderte Geschäftsordnung des Ausschusses für Beschwerde und Schlichtung wurde folgende Änderung aufgenommen:

§ 5 Abs. 5 Geschäftsordnung des Ausschusses für Beschwerde und Schlichtung

Nach Abschluss des Verfahrens vor dem Ausschuss ist sicherzustellen, dass alle fallbezogenen Unterlagen in der bei der GS geführten Verfahrensakte zusammengeführt werden. Die GS sichert die Akte mit einem Siegel und verwahrt den Vorgang unter Verschluss. Akteneinsichts- und Auskunftsrechte Betroffener oder Dritter bleiben davon unberührt.

3.4.2
Vorstellung eines neuen Rollen- und Berechtigungskonzepts zum Krankenhausinformationssystem des Klinikums Höchst

Ein Krankenhaus ist keine rechtliche Einheit, innerhalb derer personenbezogene Patientendaten beliebig offenbart werden dürfen. Auch innerhalb des Krankenhauses ist die ärztliche Schweigepflicht im Sinne der Berufsordnung und des Strafgesetzbuchs zu beachten. Das Krankenhausinformationssystem (KIS) ist so auszugestalten, dass Mitarbeiter im Krankenhaus nur Zugriff auf die Patientendaten haben, die sie tatsächlich für ihre Aufgabenerfüllung benötigen.

Ausgangspunkt war ein Datenschutzvorfall im Klinikum Höchst aus dem Jahr 2016. Damals kam es zu einem Zwischenfall auf einer Station, wo ein Patient mit einer Pistole um sich geschossen und dabei mehrere Klinikmitarbeiter verletzt hatte. Dieser veranlasste die Klinikleitung, vorsorglich eine Prüfung der erfolgten internen Zugriffe auf die elektronischen Patientenakten der betroffenen Klinikmitarbeiter vorzunehmen. Es stellte sich dabei heraus, dass eine ganze Reihe von Mitarbeiterinnen und Mitarbeitern – sowohl ärztliches wie auch pflegerisches Personal – aus verschiedenen Abteilungen unberechtigt auf die Krankenakten der verletzten Klinikmitarbeiter zugegriffen hatten.

Als Reaktion auf den Vorfall und zur Verhinderung weiterer vergleichbarer Ereignisse sicherte mir die Geschäftsleitung der Klinik zu, eine umfangreiche Anpassung des Rollen- und Berechtigungskonzepts vorzunehmen und stichprobenhafte Kontrollen der Zugriffe auf Krankenakten einzuführen. Diesen Prozess habe ich im vergangenen Jahr weiter begleitet.

Für den Umgang mit den Patientendaten der eigenen Krankenhausmitarbeiter/-innen gibt es keine speziellen gesetzlichen Regelungen. Für die Betroffenen ist es jedoch von besonderer Bedeutung, dass ihre Patientendaten geschützt bleiben und nicht Unberechtigten zur Kenntnis gelangen. Weder die Personalabteilung noch möglicherweise persönlich interessierte Kolleginnen oder Kollegen sollen die Behandlungsdaten zur Kenntnis erhalten.

Grundsätzlich dürfen im Krankenhaus Patientendaten nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind, d. h. konkret für die Durchführung des Behandlungsvertrages.

In Hessen ist im Hessischen Krankenhausgesetz 2011 (HKHG 2011) ausdrücklich vorgeschrieben, dass die in § 12 Abs. 2 HKHG 2011 festgelegten rechtlichen Voraussetzungen für die Übermittlung von Daten entsprechend auch für die Weitergabe von Patientendaten innerhalb des Krankenhauses zwischen Fachabteilungen Anwendung finden (§ 12 Abs. 3 HKHG 2011). Zugriff auf die Daten eines Patienten darf daher nur denjenigen Krankenhausmitarbeiter/-innen möglich sein, die in die Behandlung einbezogen sind oder die Behandlung verwaltungsmäßig abwickeln.

Ein Krankenhaus ist keine rechtliche Einheit, innerhalb derer personenbezogene Patientendaten beliebig offenbart werden dürfen. Auch innerhalb des Krankenhauses ist die ärztliche Schweigepflicht im Sinne der Berufsordnung und des Strafgesetzbuchs zu beachten („Inselkonzept“). So darf insbesondere eine Fachabteilung, die einen Patienten nicht behandelt, dessen detaillierte medizinische Daten nicht zur Kenntnis erhalten, es sei denn, sie übernimmt im Einvernehmen mit dem Patienten die Mit- oder Nachbehandlung. Das Verwaltungspersonal darf nur Zugriff auf Patientendaten haben, soweit dies für seine Aufgabenerfüllung und für den jeweiligen Zweck im Rahmen der Durchführung des Behandlungsvertrages erforderlich ist. Diese rechtlichen Vorgaben sind bei der Ausgestaltung der Zugriffsberechtigungen des Krankenhausinformationssystems zu beachten. Allerdings muss das entsprechende Rollen- und Berechtigungskonzept für ein Krankenhaus wegen der komplexen Aufgaben noch ausreichend Flexibilität ermöglichen (z. B. für Notfälle, Überbelegung, Nachtdienst, Verlegung, Konsil), um nicht die Patientensicherheit zu gefährden.

Umsetzung der Orientierungshilfe für Krankenhausinformationssysteme (OH KIS)

Als Orientierungsrahmen für die datenschutzkonforme Gestaltung und den datenschutzgerechten Betrieb des KIS kann die von den Datenschutzbeauftragten des Bundes und der Länder erstellte Orientierungshilfe für Kranken-

hausinformationssysteme (OH KIS) dienen (siehe auch https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Orientierungshilfe%20Krankenhausinformationssysteme.pdf). Danach muss das Rollen- und Berechtigungskonzept und dessen Umsetzung sicherstellen, dass Mitarbeiter/-innen im Klinikum nur Zugriff auf die Patientendaten haben, die sie tatsächlich für ihre Aufgabenerfüllung benötigen.

Nach der OH KIS soll es in einem KIS-System möglich sein, dass Fallakten bei Bedarf dahingehend gekennzeichnet werden können, dass der/die Patient/-in Mitarbeiter/-in des behandelnden Krankenhauses ist und dass für die Fallakte ein besonderer Schutzbedarf besteht. Die Struktur des Rollen- und Berechtigungskonzepts soll es ermöglichen, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können.

Nach den Angaben des Klinikums Höchst gibt es in der eingesetzten KIS-Software bislang keine softwaretechnische Lösung, die die Patientendaten von Mitarbeitern besonders schützt. Somit müssen, solange das eingesetzte KIS keine ausreichenden technischen Möglichkeiten bietet, entsprechend angemessene organisatorische Maßnahmen ergriffen werden, um die Patientendaten der Mitarbeiter/-innen zu schützen. Neben der Sensibilisierung der Mitarbeiter/-innen ist dabei die Protokollierung der Zugriffe im KIS und deren regelmäßige Auswertung von zentraler Bedeutung für die datenschutzgerechte Ausgestaltung des KIS. Die Protokolldaten dienen letztendlich auch zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung und zur Aufdeckung von missbräuchlichen Zugriffen oder Zugriffsversuchen. Entsprechend den Forderungen in der OH KIS muss ein Verfahren für regelmäßige, verdachtsunabhängige Kontrollen sowie für Fälle eines Verdachts auf unberechtigte Zugriffe vorgesehen sein. Dabei sind Fallakten von Mitarbeiter/-innen in einem angemessenen Umfang mit einzubeziehen. Im Interesse der Transparenz für alle Beteiligten ist das entsprechende Protokollierungs- und Auswertungskonzept den Mitarbeiter/-innen bekannt zu machen. Im Klinikum wurde mittlerweile ein entsprechendes Konzept erstellt und umgesetzt.

Da es in der Vergangenheit wiederholt zu unberechtigten Zugriffen auf Patientendaten von Mitarbeiter/-innen im Klinikum gekommen ist, war auch zu vermuten, dass es einzelnen Mitarbeiter/-innen an der entsprechenden Sensibilität für den Datenschutz mangelt. Ich habe die Klinik aufgefordert, geeignete Maßnahmen zu ergreifen, um das Datenschutzbewusstsein der Mitarbeiter/-innen zu verbessern. Die Klinik hat darauf reagiert und entsprechende Informationen und Rundschreiben verschickt. Weiterhin sind die Mitarbeiter/-innen verpflichtet, regelmäßig an Datenschutzschulungen teilzunehmen. Zusätzlich erfolgen abteilungsspezifische Schulungen zu

Datenschutzthemen, um auf Besonderheiten in der jeweiligen Arbeitseinheit einzugehen.

Zwischenzeitlich hat mir die Klinik erste Teile eines überarbeiteten Zugriffskonzepts vorgestellt, in dem die Möglichkeiten von unberechtigten Zugriffen auf Patientendaten weiter reduziert werden können:

– Um zukünftig in Notfällen trotz der eingeschränkten Zugriffsberechtigungen auf Patientendaten außerhalb des eigentlichen Zuständigkeitsbereichs zugreifen zu können, wird ein Notfallzugriff eingerichtet. Jeder Zugriff über diese Funktion ist vom Nutzer zu begründen und wird dokumentiert. Monatlich erfolgt eine stichprobenhafte Prüfung und Auswertung der erfolgten Zugriffe.
– Weiterhin wurde die bislang klinikweite Patientensuchfunktion eingeschränkt.
– Um eine unbefugte Nutzung des KIS durch Dritte auszuschließen, erfolgt zukünftig eine automatische Abmeldung des Mitarbeiters vom KIS bei längerer Inaktivität.

Die Diskussion über einige Bereiche ist aktuell noch nicht abgeschlossen. So hat man mir zugesagt, auch weiter an einer technisch befriedigenden Umsetzung eines Konzepts zum Schutz von VIPs oder Mitarbeitern, die sich in Behandlung befinden, zu arbeiten. Ich werde die diesbezüglichen Entwicklungen weiterverfolgen.

3.4.3
Einsichtnahme in die Patientenakte durch Erben und Angehörige nach dem Tod des Patienten

Erben und Angehörige haben im Fall des Todes der Patientin oder des Patienten ein Recht auf Einsicht in die Patientenakte der oder des Verstorbenen unter den Voraussetzungen des § 630g Abs. 3 BGB. Immer wieder zeigt sich jedoch, dass Ärzteschaft und Krankenhäuser nicht rechtssicher mit dem Anspruch umgehen.

In der ersten Jahreshälfte gingen in meiner Behörde mehrere Beschwerden darüber ein, dass Angehörigen verstorbener Patientinnen und Patienten Akteneinsicht in die Patientendokumentation verwehrt wurde. In einem Fall handelte es sich um die Schwester einer verstorbenen Patientin, in einem weiteren um die Tochter des Verstorbenen. Beide beriefen sich gegenüber den Krankenhäusern auf ihr Recht aus § 630g Abs. 3 BGB als Angehörige. Ein immaterielles Interesse wurde jeweils vorgetragen.

§ 630g BGB

(1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren. …

…

(3) Im Fall des Todes des Patienten stehen die Rechte aus den Absätzen 1 und 2 zur Wahrnehmung der vermögensrechtlichen Interessen seinen Erben zu. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen. Die Rechte sind ausgeschlossen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten entgegensteht.

Die Einsicht wurde aus vielerlei Gründen verwehrt.

Der Schwester gegenüber machte das Krankenhaus u. a. geltend, sie sei keine „nächste Angehörige", es würden wohl noch Kinder und der Ehemann der verstorbenen Schwester leben, die in der Rangfolge vor ihr kämen. Sollten diese verstorben sein, stünde der Schwester ein Recht auf Einsicht zu.

Von der Tochter des Verstorbenen wurde zunächst ein Erbschein verlangt. Sollte dieser dem Krankenhaus als Nachweis der Erbschaft vorgelegt werden, würde die Kopie der Akte ohne weitere Nachfrage übersandt werden. Als die Tochter sich mangels eines Erbscheins auf ihr Recht als Angehörige berief, wurde ihr entgegnet, die Unterlagen könnten nur mit vermutetem Einverständnis des verstorbenen Patienten zur Verfügung gestellt werden. Ein solches müsse von ihr belegt werden.

Das in § 630g BGB normierte Recht des Patienten auf Einsicht in die ihn betreffende Patientenakte dient nach der Gesetzesbegründung der Verwirklichung seines Rechts auf informationelle Selbstbestimmung (BTDrucks. 17/10488, S. 26). Trotz des zivilrechtlichen Charakters der Norm ist diese auch datenschutzrechtlich relevant.

Zum Begriff der „nächsten Angehörigen" habe ich die Position bezogen, dass von einer Rangfolge der in der Gesetzesbegründung genannten Angehörigen (Ehegatten, Lebenspartner, Kinder, Eltern, Geschwister und Enkel) nicht auszugehen ist. Das Fehlen einer ausdrücklichen Bestimmung zur Rangfolge spricht dafür, dass eine solche nicht vorgesehen ist und somit alle nächsten Angehörigen gleichermaßen bei Vorliegen eines immateriellen Interesses zur Einsichtnahme berechtigt sind. Hierin unterscheidet sich die Vorschrift des § 630g Abs. 3 BGB etwa von den Vorschriften des Transplantationsgesetzes (TPG), das in § 1a Nr. 5 ausdrücklich eine Rangfolge bestimmt und in den folgenden Vorschriften jeweils nur von einem nächsten Angehörigen spricht (vgl. § 3 Abs. 3 TPG, § 4 Abs. 1 und 2 TPG) oder von § 77 Abs. 2 StGB, der ebenfalls eine Rangfolge der antragsberechtigten Angehörigen vorgibt. Der Wortlaut des § 630g Abs. 3 BGB bestimmt „die nächsten Angehörigen" als an-

spruchsberechtigt. Wäre der Gesetzgeber von einer Rangfolge ausgegangen, hätte er „den nächsten Angehörigen“ als Anspruchsberechtigten bestimmt.

Zudem habe ich im zweiten Fall darauf hingewiesen, dass die Beweislast für einen entgegenstehenden Willen die behandelnde Person trägt. Nicht die Angehörigen bzw. die Erben müssen mithin darlegen und beweisen, dass die oder der Verstorbene mit einer Einsicht einverstanden gewesen wäre, sondern die oder der Behandelnde muss in Grundzügen darlegen und beweisen, dass der Einsichtnahme der ausdrückliche oder mutmaßliche Wille der oder des Verstorbenen entgegensteht. Dies ergibt sich schon aus dem Wortlaut des § 630g Abs. 3 Satz 3 BGB und soll – unter Berücksichtigung des Schutzes des Patienten in Bezug auf die in der Patientenakte enthaltenen Informationen auch über seinen Tod hinaus – dem Grundsatz Rechnung tragen, dass es im Normalfall dem Willen des Patienten entspricht, dass nach seinem Tod Erben und Angehörige die Patientenakte im gesetzlich definierten Umfang einsehen.

Den beiden Angehörigen wurde daraufhin von den Krankenhäusern Einsicht gewährt. Aufgrund der zahlreichen zu Tage getretenen Unsicherheit im Umgang mit dem § 630g Abs. 3 BGB habe ich die in den Fällen relevanten Fragestellungen zusammengefasst und ein Informationspapier für meine Homepage erstellt (https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/einsichtnahme-die-patientenakte-durch-erben).

3.5
Technik, Organisation

3.5.1
Angriffsszenarien Spectre und Meltdown: Was bedeuten sie für virtualisierte Umgebungen?

Seit mehreren Jahren ist auf Unternehmensseite ein anhaltender Trend zur Virtualisierung von IT-Infrastrukturen und zur Verlagerung von Diensten und Applikationen in die Cloud zu beobachten. Am 03.01.2018 wurden unter den Namen Spectre und Meltdown zwei Arten von Angriffsszenarien auf gravierende Schwachstellen in modernen Prozessorarchitekturen veröffentlicht. Hiervon sind in großem Umfang virtualisierte Umgebungen betroffen, sodass aus Sicht des Datenschutzes eine Analyse möglicher Auswirkungen und resultierender Risiken als Grundlage für eine angemessene Risikobewertung unerlässlich ist.

Virtualisierung und Cloud-Computing

Virtualisierung und Cloud-Computing sind zwei eng miteinander verknüpfte, weit verbreitete und populäre Trends im Kontext heutiger IT-Landschaften.

Hierbei kommt häufig eine Virtualisierung als Grundlage des Cloud-Computing zum Einsatz. Ein wesentliches Konzept der Virtualisierung ist die gemeinsame Nutzung von Hardware-Ressourcen bei gleichzeitiger Abgrenzung der nutzenden Software-Systeme untereinander. Einem Software-System wird hierbei eine virtuelle Umgebung exklusiv zur Verfügung gestellt. Mehrere virtuelle Umgebungen können auf Basis ein und derselben Hardware-Plattform parallel und voneinander separiert betrieben werden. Durch die Separierung werden virtuelle Umgebungen derart isoliert, dass unerwünschte Wechselwirkungen, etwa der wechselseitige Zugriff auf Daten, unterbunden werden. Durch solche Maßnahmen wird u. a. das Ziel einer Mandantentrennung verfolgt. Aus Sicht des Betreibers von Virtualisierungsplattformen lassen sich Hardware-Ressourcen insbesondere dann effizient einsetzen, wenn auf ihnen mehrere virtuelle Umgebungen gleichzeitig zum Einsatz kommen. Neben wirtschaftlichen Aspekten werden hierdurch auch Forderungen an eine Green IT erfüllt.

Grundlage der Virtualisierung ist eine Trennung in die wesentlichen Komponenten Wirt und Gast. Ein Wirt übernimmt vor allem die Kernaufgabe der Verwaltung von Ressourcen. Er stellt Gästen virtuelle Gast-Umgebungen zur Verfügung und übernimmt die Zuteilung der verfügbaren Ressourcen an diese Gast-Umgebungen. Gäste nutzen die ihnen zugeteilte virtuelle Umgebung zur Erfüllung ihrer Aufgaben. Die folgende Abbildung zeigt diese Struktur schematisch.

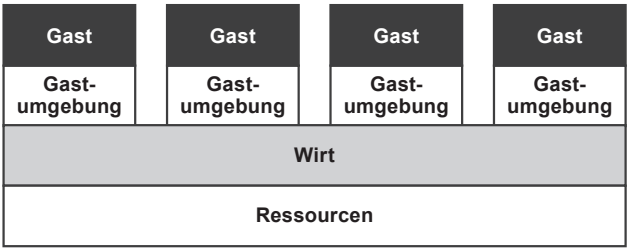


Abbildung: Grundaufbau virtualisierter Umgebungen

In der Praxis kommen unterschiedliche Virtualisierungsarten vor. Prominente Vertreter sind die Hardware- und die Betriebssystem-Virtualisierung. Bei der Hardware-Virtualisierung stellt der Wirt dem Gast eine virtuelle Maschine als Gast-Umgebung zur Verfügung, welche dieser i. d. R. zunächst als Basis für die Installation und Konfiguration eines Betriebssystems verwendet. Anschließend erfolgen weiterführende Aktivitäten gemäß dem beabsichtigten Einsatzzweck, etwa die Installation, Konfiguration und Inbetriebnahme

von Diensten. Die Betriebssystem-Virtualisierung verfolgt den Ansatz der gemeinsamen Nutzung eines Betriebssystems durch Gäste. Während das Basis-Betriebssystem bzw. dessen Kern gemeinsam genutzt wird, können darauf aufbauende Komponenten, z. B. Bibliotheken, Gästen zur Verfügung gestellt und durch diese exklusiv genutzt werden. Die Bereitstellung der Gastumgebung erfolgt hierbei in Form eines sogenannten Containers.

Eine wesentliche Anforderung beim Einsatz von Virtualisierungsplattformen ist, aus Sicht des Datenschutzes, eine uneingeschränkte Isolation der virtuellen Umgebungen untereinander. Eine solche Isolation ist grundlegend für eine Mandantentrennung, die wiederum Voraussetzung einer datenschutzkonformen Verarbeitung von personenbezogenen Daten ist. Dies gilt umso mehr, falls sich Umgebungen unterschiedlicher Nutzer ein und dieselbe Hardware-Plattform teilen, etwa im Kontext der Plattform eines Cloud-Dienstleisters (Public Cloud). Andernfalls könnten sich potenziell unkalkulierbare Risiken für Gewährleistungsziele, wie Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettbarkeit, ergeben.

Rollen

Im Kontext virtualisierter Umgebungen sind unterschiedliche Rollen mit entsprechenden Verantwortlichkeiten zu berücksichtigen. Diese lassen sich in die zwei Gruppen Hersteller und System-Betreibende unterteilen.

In der Gruppe der Hersteller sind diejenigen Rollen zusammengefasst, die Hardware oder Software als Grundlage virtueller Architekturen bereitstellen. Entsprechend lässt sich die Gruppe der Hersteller weiter in Hardware- und Betriebssystem-Hersteller sowie Hersteller von Virtualisierungssoftware unterteilen.

In der Gruppe der System-Betreibenden sind Plattform-Betreibende und Gast-Betreibende zusammengefasst. Erstere setzen eine Kombination aus Hardware und Software ein, um eine Virtualisierungsplattform bereitzustellen und dauerhaft zu betreiben. Letztere nutzen eine vom Plattform-Betreibenden auf Basis seiner Virtualisierungsplattform bereitgestellte virtuelle Umgebung, um hierauf aufbauend die von ihm gewünschten Anwendungen und Dienste bereitzustellen.

Es ist hervorzuheben, dass durchaus mehrere Rollen von ein und demselben Akteur wahrgenommen werden können. So kann bspw. ein Unternehmen eine eigene Virtualisierungsplattform (Private Cloud) betreiben und auf Basis dieser Dienste bereitstellen. In diesem Szenario würde das Unternehmen sowohl die Rolle des Plattform-Betreibenden als auch die des Gast-Betreibenden einnehmen.

Komplexe IT-Landschaften

In den beiden vorangegangenen Kapiteln wurden virtuelle Umgebungen und Rollen dargestellt. Dabei wurde auf eine einzelne physische Umgebung und deren Hardware-Ressourcen fokussiert. Plattform-Betreibende verfügen in ihrer jeweiligen Plattform-Landschaft jedoch in der Regel über mehrere physische Umgebungen. Diesen ordnen sie Gast-Umgebungen zu. Die Menge der einem Gast zur Verfügung gestellten virtuellen Umgebungen und der Verbindungen zwischen diesen bilden entsprechend eine Gast-Landschaft.

Bisher wurde jeweils von genau einem Gast-Betreibenden und genau einem Plattform-Betreibenden ausgegangen. Diese Situation ist jedoch häufig so nicht gegeben:

Ein Unternehmen kann virtuelle Umgebungen bei unterschiedlichen, unternehmensexternen Plattform-Betreibenden, etwa in einer Public Cloud, anmieten. Gleichzeitig kann das Unternehmen selbst intern als Plattform-Betreibender mit eigenem Rechenzentrum auftreten. Im Kontext öffentlicher Virtualisierung-Plattformen kommt es darüber hinaus häufig zu Situationen, in denen virtuelle Umgebungen unterschiedlicher Gäste auf derselben physischen Umgebung eines Cloud-Dienstleisters betrieben werden.

Im Ergebnis sind im praktischen Einsatz häufig komplexe IT-Landschaften mit einer Vielzahl von Akteuren in unterschiedlichen Rollen anzutreffen. Dies gilt insbesondere für Public Clouds.

Auswirkungen

Sofern eine uneingeschränkte Mandantentrennung der einzelnen virtuellen Umgebungen untereinander sowie in Bezug auf Verbindungen zwischen diesen gewährleistet ist, ist aus Gast-Sicht eine Fokussierung auf die eigene virtuelle Gast-Landschaft ausreichend. Dies ist aus Sicherheitsgesichtspunkten möglich, da in einem solchen Szenario eine vollständige Abgrenzung der Gast-Umgebungen und -Landschaften sichergestellt ist.

Durch die von Spectre und Meltdown ausgenutzten Schwachstellen in modernen Prozessorarchitekturen ist das unberechtigte Auslesen von Speicherbereichen und somit von Daten auf Hardware-Ebene möglich. In Bezug auf die vorangegangenen Erläuterungen zur Virtualisierung und zum Cloud-Computing bedeutet dies, dass die unterste Ebene der skizzierten Architekturen betroffen ist. Auf dieser Ebene werden Ressourcen bereitgestellt, die auf darüber liegenden Ebenen an Gast-Umgebungen vergeben werden. Dementsprechend besteht, sofern die zugrundeliegende Hardware von den Schwachstellen betroffen ist, grundsätzlich die Gefahr eines Ausspähens von Daten über die Grenzen von Gast-Umgebungen hinweg. Dies gilt für

Gast-Umgebungen, die auf Basis derselben physischen Umgebung bereitgestellt werden. In einem solchen Fall ist die zentrale Anforderung der Isolation virtueller Umgebungen untereinander nicht mehr sichergestellt. Zusätzlich kann auch die Abgrenzung zwischen der physischen Umgebung auf der einen und den virtuellen Umgebungen auf der anderen Seite betroffen sein.

Schlussfolgerungen

Das Gefahrenpotenzial für einzelne, auf Basis virtueller Umgebungen betriebene Verfahren hängt von mehreren Faktoren ab. Grundsätzlich ist zum Ausnutzen der Schwachstellen die Möglichkeit zur Programmcodeausführung erforderlich. Zu beachten ist hierbei, dass die Ausführung nicht unbedingt innerhalb der betrachteten virtuellen Umgebung erfolgen müsste. Vielmehr könnte, bedingt durch die aufgebrochene Isolation, ein entsprechender Programmcode in einer virtuellen Umgebung ausgeführt werden, um eine andere virtuelle Umgebung innerhalb derselben physischen Umgebung auszuspähen. Virtuelle Umgebungen können folglich bei der Risikoanalyse und -bewertung nicht isoliert betrachtet werden.

In einer privat betriebenen oder dediziert bereitgestellten physischen Umgebung liegen Informationen über deren virtuelle Umgebungen vor. Für all diese virtuellen Umgebungen muss das Risiko der Programmcodeausführung zu Ausspähzwecken betrachtet und bewertet werden. Hierbei muss von der Annahme ausgegangen werden, dass die gefährdetste virtuelle Umgebung die Risikobewertung der übrigen Umgebungen bestimmt. Zusätzlich müssen Maßnahmen ergriffen werden, um relevante Änderungen im Zeitablauf zu identifizieren und zu berücksichtigen. Hierzu zählen insbesondere auch Änderungen bei der Zuordnung von virtuellen Umgebungen zu den zugrundeliegenden physischen Umgebungen. In den vorangegangenen Szenarien wurde implizit davon ausgegangen, dass ein Angreifer sich Zugriff auf eine virtuelle Umgebung verschaffen muss, um den für das Ausspähen notwendigen Programmcode auszuführen. Zu beachten ist hierbei, dass ein solcher Zugriff nicht zwingend einen Angriff auf eine virtuelle Maschine voraussetzt. Ein denkbares Szenario wäre auch das Anmieten einer virtuellen Umgebung in einer Public Cloud mit dem Ziel, diese zu Angriffszwecken auf benachbarte Umgebungen derselben physischen Umgebung zu verwenden. Eine datenschutzrechtliche Anforderung kann daher auch die exklusive Verwendung von dedizierter Hardware für bestimmte Verfahren sein.

Zusammenfassend ist festzustellen, dass die durch die Veröffentlichung von Spectre und Meltdown aufgedeckten Schwachstellen tiefgreifende Auswirkungen auf Risikobetrachtungen von virtualisierten Umgebungen und Landschaften haben. Damit ist eine zentrale Anforderung des Datenschutzes,

die umfassende und wirksame Isolation virtueller Gast-Umgebungen und Verbindungen zwischen diesen, nicht mehr uneingeschränkt erfüllt. Konsequenzen hieraus ergeben sich auf allen Ebenen der zugrundeliegenden Architekturen und für alle beteiligten Akteure. Der Hessische Datenschutzbeauftragte hat am 11.01.2018 eine Pressemitteilung herausgegeben, in der er alle Akteure zur Ergreifung notwendiger Maßnahmen aufgefordert hat. Die Pressemitteilung kann von der Website des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unter https://datenschutz.hessen.de/pressemitteilungen/spectre-und-meltdown abgerufen werden.

3.5.2
Einführung der App „BAföGdirect“

Bereits im 41. Tätigkeitsbericht (Ziff. 3.3.3.2) und im 44. Tätigkeitsbericht (Ziff. 3.2.1) habe ich mich ausführlich mit dem Hessisches BAföG-/AFBG-Verfahren beschäftigt. Es gehörte von Anfang an zu den modernsten Verfahren in Deutschland. Mit der Einführung der App „BAföGdirect“ ist Hessen abermals Vorreiter. Ab Mai 2018 sind damit Services rund um den Antrag auf Leistungen für Smartphone und Tablet optimiert möglich.

Die Firma Datagroup IT Solutions GmbH hat als Dienstleister des HMWK für das IT-Fachverfahren (BAföG- und AFBG-Software inkl. Betrieb) als weitere Ausbaustufe des bestehenden Vertrages des seit Mai 2012 unter https://www.bafög-hessen.de vorhandenen Online-Antragangebotes eine App für BAföG (Studierende und Schüler/-innen) und Aufstiegs-BAföG (AFBG) entwickelt. Die Entwicklung wurde durch das HMWK und meine Mitarbeiter begleitet.

Die App „BAföGdirekt“ unterstützt die bisherigen Features der Online-Beantragung im BAföG und AFBG auf Smartphone und Tablet und wurde am 25.01.2018 in Hessen eingeführt.

Folgende Dienstleistungen werden durch die App mobil ermöglicht:

– Das zuständige Amt und dessen Kontaktdaten können ermittelt werden, eine Kontaktaufnahme kann direkt aus der App heraus erfolgen (durch Anruf oder per E-Mail).
– Die App enthält eine „Navigationsfunktion“. Diese ermöglicht den Nutzern, nach Ermittlung des zuständigen Amtes direkt die Route zur Besucheranschrift abhängig vom verwendeten Endgerät in Google Maps bzw. Apple Maps berechnen und anzeigen zu lassen.
– Die Statusabfrage zum Stand der Antragsbearbeitung kann passiv erfolgen, in dem bei einer Statusänderung in der Antragsbearbeitung – nach expliziter Zustimmung durch den Nutzer im Rahmen der Installation der

App – eine Pushmitteilung automatisiert übermittelt wird. Diese Funktion kann vom Nutzer jederzeit aktiviert oder deaktiviert werden.

– Wesentliche Neuerung: Dokumente können zur Übermittlung mit dem Smartphone oder Tablet fotografiert und direkt und sicher an das zuständige Amt übermittelt werden. Dadurch kann auf das bislang erforderliche Einscannen und Hochladen für eine Übermittlung im Dokumenten-Uploadportal verzichtet werden. Die Dokumente werden ins Fachverfahren übertragen, ein wichtiger weiterer Schritt auf dem Weg hin zur Digitalisierung von Verwaltungsleistungen und der elektronischen Akte.

Die App unterstützt die Betriebssysteme iOS (Apple) und Android (google). Damit können derzeit 97 % aller Smartphone-Besitzer in Deutschland diese Dienstleistung nutzen.

Die App ist ein wichtiger weiterer Beitrag zur Strategie „Digitales Hessen 2020“. Das „Hessische BAföG und AFBG-Verfahren (HeBAV)“ ist darin in Teil II unter 3.10 benannt.

Zum einen dient die Erweiterung des bestehenden Onlineangebotes um die App dem weiteren Ausbau der Dienste für Bürger (E-Services) und zum anderen trägt sie zur Optimierung der Verwaltungsprozesse (E-Administration) bei, weil darüber übermittelte Dokumente vom Amt direkt in die sich im Aufbau befindliche elektronische Akte übernommen werden können. Es wird erwartet, dass durch dieses zeitgemäße Feature die BAföG- und AFBG-Antragsteller verstärkt angesprochen und insbesondere von der mobilen Funktion der Dokumentenübermittlung Gebrauch machen werden.

Hessen ist das erste Bundesland, das seinen Antragstellern im BAföG und AFBG (Studierenden, Schülerinnen und Schülern sowie Teilnehmenden an Fortbildungsmaßnahmen) eine solche Dienstleistung anbietet.

3.5.3
Bürger- und Unternehmensservice Hessen

Das Onlinezugangsgesetz sieht vor, dass alle Verwaltungsdienstleistungen über das Internet angeboten werden sollen. Ein Infrastrukturbaustein für die Angebote sowohl der Kommunen als auch des Landes ist das Angebot von interoperablen Nutzerkonten. Hier baut Hessen auf die Vorarbeiten des Bürger- und Unternehmensservice Hessen (BUS Hessen) auf.

Die Vorgaben des Onlinezugangsgesetzes

Das Onlinezugangsgesetz (OZG) vom 14.08.2017 trat am 18.08.2017 in Kraft.

In § 1 Abs. 1 OZG werden alle Behörden von Bund und Ländern verpflichtet, ihre Verwaltungsleistungen binnen fünf Jahren (bis 2022) auch elektronisch und über Verwaltungsportale zur Verfügung zu stellen. Nach § 1 Abs. 2 OZG müssen Bund und Länder ihre Verwaltungsleistungen in einem Portalverbund miteinander verknüpfen.

§ 3 Abs. 2 OZG verpflichtet Bund und Länder, Nutzerkonten im Portalverbund bereitzustellen. Nach § 7 OZG bestimmen Bund und Länder öffentliche Stellen, die die Einrichtung und Registrierung von Nutzerkonten vornehmen. Daran ist ersichtlich, dass ein wesentliches Ziel des OZG die Bereitstellung von interoperablen Nutzerkonten für einen einheitlichen, komfortablen und sicheren Zugang zu online angebotenen Verwaltungsleistungen ist. Das gilt für die Kommunal-, Landes- oder Bundesebene.

Ein OZG-Umsetzungskatalog kommt als Ausgangsbasis für die Erfassung/Kartierung der Verwaltungsleistungen zum Einsatz:

– 575 umzusetzende Leistungsbündel
  gegliedert in 55 Lebenslagen und Geschäftslagenpaket (wobei jedes dieser Pakete durchschnittlich zehn Verwaltungsleistungen enthält) bzw. 1981 aktuell in Hessen umzusetzende Leistungen.

Der Katalog soll laufend aktualisiert und fortgeschrieben werden.

Über das Hessische Gesetz zur Förderung der elektronischen Verwaltung (Hessisches E-Government-Gesetz – HEGovG) werden auch die Kommunen verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente zu schaffen (§ 1 Abs. 1 Nr. 1 i. V. m. § 3 Abs. 1 HEGovG).

§ 3 Abs. 1 HEGovG

Jede Behörde ist verpflichtet, einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen.

Die Umsetzung des OZG in Hessen

Um die genannten Anforderungen zu erfüllen, wurde durch die Hessische Landesverwaltung u. a. das Projekt „Umsetzung OZG“ ins Leben gerufen. Das Projekt ist als Vorprojekt im HMDIS angesiedelt.

Im Projekt „Umsetzung OZG“ sollen die notwendigen organisatorischen, inhaltlichen, zeitlichen und finanziellen Konkretisierungen erarbeitet werden. Diese bilden die Grundlage einer Strategie zur Umsetzung des OZG bis Ende

des Jahres 2022. Wesentliche Ziele und Rahmenbedingungen des Projekts sind u. a. folgende Punkte:

– Aufarbeiten der rechtlichen, politischen und organisatorischen Rahmenbedingungen auf EU-, Bundes- und Landesebene (beinhaltet die Kommunen),
– Beantwortung rechtlicher Fragestellungen sowie Fragen bzgl. des Datenschutzes bei Land und Kommunen, u. a. zur rechtlichen Verankerung der OZG-Aktivitäten im Rahmen des HEGovG.
– Die Umsetzung der einzelnen Fachverfahren soll dezentral erfolgen und durch die Ressorts gesteuert werden.
– Alle Verwaltungsleistungen i. S. d. OZG sind ja bereits vorhanden und gründen sich auf Rechtsnormen, d. h. auf ein breites Spektrum von Bundesgesetzen, Landesgesetzen, Richtlinien und Verordnungen bis hin zu kommunalen Satzungen und Subventionsrichtlinien im Sinne von Verwaltungsvorschriften.
– Teilweise sind die Leistungen auch schon online zugänglich. In Hessen trifft dies aktuell auf 13 % der kommunalen Leistungen zu.
– Zuständig für die Pflicht zur Einhaltung der Datenschutzvorschriften der DS-GVO und des HDSIG bei der Verarbeitung von personenbezogenen Daten sind die Verantwortlichen.
– Im öffentlichen Bereich ist Verantwortlicher die jeweiligen Daten verarbeitende öffentliche Stelle im Sinne von § 2 Abs. 1 HDSIG, also wie bisher z. B. die Gemeinde oder das Ministerium. Die Letztverantwortlichkeit verbleibt dabei nach der DS-GVO bei der Behördenleitung bzw. der Leitung der öffentlichen Stelle.

Die jeweiligen Verantwortlichen und Auftragsverarbeiter haben eine zentrale Verantwortung, insbesondere für

– die Zulässigkeit der Verarbeitung der personenbezogenen Daten,
– die Beachtung der Verfahrensvorschriften, d. h. das Führen von Verzeichnissen der Verarbeitungstätigkeiten, Melde- und Benachrichtigungspflichten und die Durchführung von Datenschutz-Folgenabschätzungen sowie
– die technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten Daten.

Bei der Analyse der Ausgangslage waren nicht zuletzt die rechtlichen Rahmenbedingungen sowie Fragen bzgl. Datenschutz bei Land und Kommunen einzubeziehen. Da gerade die Bereitstellung von interoperablen Nutzerkonten eine wichtige Komponente des Systems sein wird, hatte man sich entschlos-

sen, auf die Vorarbeiten der Entwicklung des Bürger- und Unternehmensservice (BUS) Hessen zurückzugreifen.

Entwicklung des Bürger- und Unternehmensservice (BUS) Hessen

Bereits Mitte 2015 hatte sich der IT-Planungsrat für eine flächendeckende Verbreitung von Servicekonten für Bürger und Unternehmen ausgesprochen. Nach einer gründlichen Prüfung der rechtlichen Rahmenbedingungen, wie beispielsweise das EGovG des Bundes, hatte das HMDIS Mitte 2016 Grundsätze formuliert, aus denen sich insbesondere ergab, welche Daten zu diesem Zweck verarbeitet werden dürfen.

Die hessische Landesverwaltung hat dann die Strategie „Digitales Hessen" entwickelt, in der u. a. die Dienstleistungen für Bürger und Unternehmen (e-Services) untersucht wurden. Dabei wurden die EU-Verordnung zur Errichtung eines zentralen digitalen Zugangstors (Single Digital Gateway) und der Entwurf des OZG berücksichtigt. Zu den unverzichtbaren Komponenten gehörte der Identitätsbaustein „Servicekonto mit Postfach", der als Servicekonto im BUS-Hessen firmierte. Anfang 2018 stellte sich die Lage wie folgt dar:

– Interoperable Servicekonten werden auf der Ebene der Länder gehalten und sind als Nutzerkonten im OZG beschrieben.
– Interoperable Servicekonten existieren in der Ausprägung: Bürgerkonten für natürliche Personen oder Unternehmenskonten für juristische Personen.
– Interoperable Servicekonten haben interoperable Postfächer.
– Interoperable Servicekonten können an einen Payment-Serviceprovider angebunden werden.
– Die Interoperabilität wurde mit Erfolg getestet.
– Das interoperable Servicekonto Hessen nutzt die Technologie, die von dem Rechenzentrum AKDB der bayerischen Kommunen bereitgestellt wird, und wird bei der ekom21 installiert.
– Ein Kooperationsvertrag Bund/Bayern/Hessen ist abgeschlossen.

Im Folgenden wurden für das Servicekonto eine Muster-Vorabkontrolle durchgeführt und ein Muster-Verfahrensverzeichnis erstellt. Diese wurden mir vorgestellt. Nach meinen Anmerkungen wurde die Vorabkontrolle überarbeitet.

Potenzielle Nutzer, nämlich Bürgerinnen und Bürger (aktuell in Hessen ca. 5 Mio.) sowie Unternehmen (aktuell in Hessen ca. 260.000), sollen nach § 3 OZG und § 3 Abs. 4 HEGovG Nutzerkonten (früher Servicekonto genannt) einrichten können. Hierbei wird – einmalig – ein Kerndatensatz hinterlegt, der

bei einer Inanspruchnahme der Verwaltungsleistungen zum Einsatz kommt (Once-Only-Prinzip).

Die unterschiedlichen öffentlichen Stellen sollen über Schnittstellen auf das Nutzerkonto zugreifen und die erforderlichen Daten für ein Fachverfahren abrufen, soweit sie dazu autorisiert sind.

Nach § 7 Abs. 1 OZG bestimmen Bund und Länder jeweils eine öffentliche Stelle, die den Nutzern die Einrichtung eines Nutzerkontos im Portalverbund anbietet. Nach Festlegung des BMI ist damit nicht alleine die Zuständigkeit für die technische Einrichtung und Zurverfügungstellung des Nutzerkontos gemeint, sondern auch die datenschutzrechtliche Verantwortung für dieses Konto.

§ 7 Abs. 1 OZG sagt also u. a. aus, dass die von Bund und Ländern bestimmten Stellen die Verantwortung für die Einhaltung des Datenschutzes tragen, soweit das Nutzerkonto betroffen ist. Von dieser Festlegung können die EGovG der Länder nicht wirksam abweichen, da das OZG diesbezüglich auch für die Länder verbindlich ist. In Hessen wurde die ekom21 als diese Stelle bestimmt.

Technische Einbindung des Nutzerkontos/Servicekontos im BUS-Hessen

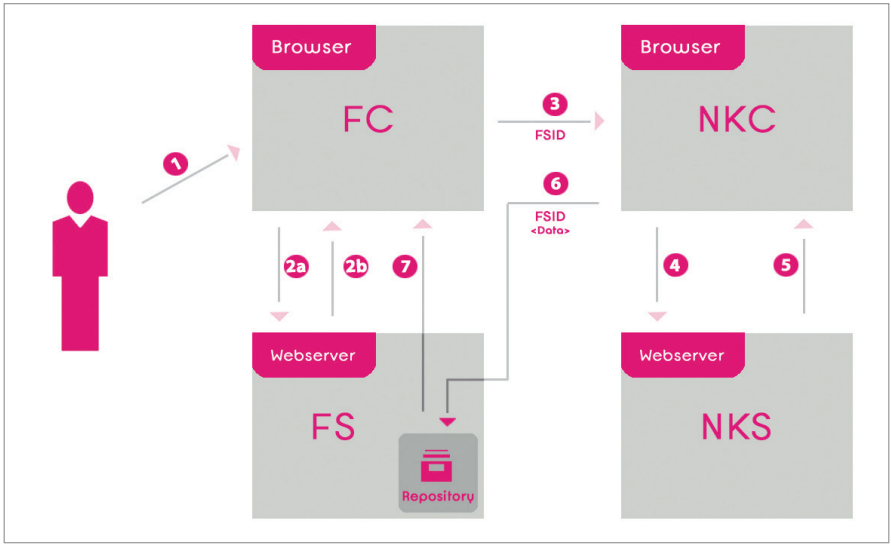
Zum Datenabruf berechtigte Verwaltungsdiensteanbieter werden von der ekom21 – KGRZ Hessen jeweils unter Angabe von

– EntiyID,
– Rücksprungadresse,
– X509-Zertifikat

geprüft, registriert und eingerichtet.

Es werden abhängig von den für den Service benötigten Daten nur die hierfür erforderlichen Attribute zum Datenabruf bereitgestellt.

Der technische Ablauf des Datenabrufs stellt sich wie folgt dar:



Legende:

FC:	Fachverfahren-Client
FS:	Fachverfahren-Server
NKC:	Nutzerkonto-Client
NKS:	Nutzerkonto-Server
FSID:	ID des Fachverfahrens/Services

Kommunikationswege:

1 Aufruf der Webseite des Service durch einen Externen (z. B. einen Bürger)

2a Abruf der Seite vom Fachverfahrensserver

2b Rückgabe der notwendigen Informationen über die vom Fachverfahren (Verwaltungsdienst) notwendigen Attribute aus Nutzerkonto und TransaktionsID/VerfahrensID und Übermittlung der notwendigen Authentifizierungsstufe

3 Aufruf der Loginseite des Nutzerkontos (Aufruf in einem Popup oder in einer separaten Seite) und Übergabe der TransaktionsID/VerfahrensID sowie der notwendigen Attribute

4 Validierung der Logindaten gegen das Nutzerkonto

5 Rückgabe der TransaktionsID/VerfahrensID und der notwendigen Attribute

6 Aufruf des Fachverfahrensservers mit Übergabe TransaktionsID/VerfahrensID und der angeforderten Attribute

7 Rückgabe der neuen Seite des Fachverfahrens

Die Abläufe bedeuten, dass jeder Bürger sich beim einzelnen Aufruf entscheiden kann, ob er das Nutzerkonto einsetzen möchte.

Fazit

Es werden damit die Voraussetzungen geschaffen, Portale mit einem datenschutzgerechten Identitätsnachweis zu nutzen.

3.6
Arbeitsstatistik (bis 24.05.2018)

3.6.1
Eingaben und Beratungen

Die Tätigkeit praktisch aller meiner Mitarbeiterinnen und Mitarbeiter (Geschäftsstelle, IT-Abteilung und Rechtsabteilungen) war bis 24.05.2018 weithin von den 2017 begonnenen Vorbereitungen auf die Anforderungen der Europäischen Datenschutzreform geprägt.

Hausintern untersuchten in über 35 Teilprojekten einzelne Arbeitsgruppen spezifische Themen der DS-GVO auf ihre Auswirkungen im Verwaltungsvollzug. Aufgabe der einzelnen Arbeitsgruppen war es insbesondere herauszuarbeiten, welche rechtlichen, technischen und/oder organisatorischen Maßnahmen zur Vorbereitung auf das neue Recht zu treffen waren. Auf diese Weise konnten erste Anwendungs- und Verständigungsfragen von verantwortlichen Datenverarbeitern, internen Datenschutzbeauftragten, Bürgerinnen und Bürgern sowie Anfragen aus der Politik und den Medien zuverlässig beantwortet werden.

In vielen Arbeitssitzungen wurden, nicht nur behördenintern, sondern auch auf Länder-, Bund- und EU-Ebene, Auslegungs-, Abstimmungs- und Organisationsfragen diskutiert und nach Möglichkeit geklärt, Meinungsbildungsprozesse eingeleitet und Orientierungshilfen bzw. Leitlinien festgelegt, um zum Stichtag der DS-GVO erste Ergebnisse für eine einheitliche Anwendung der DS-GVO präsentieren zu können. Die notwendigen organisatorischen Vorgaben, wie z. B. Einführung eines Fristensystems, Erneuerung der Homepage mit Bereitstellung eines elektronischen Zugangs für Datenschutzbeschwerden und Datenschutzpannen, konnten fristgerecht umgesetzt werden. Auf der Homepage wurden zahlreiche Beiträge und Anwendungshinweise (z. B. aus dem Schulbereich oder Gesundheitswesen) zusammengetragen, um Nutzern eine erste Orientierung anzubieten. Diese Vorbereitungsmaßnahmen erfolgten neben der alltäglichen Facharbeit. Was letztere angeht, so war die Anzahl der Eingänge von Beschwerden und Beratungsanfragen in den

ersten Monaten noch ähnlich wie im Vorjahr. Bis zum Stichtag 25.05.2018 wich die Statistik trotz erster Nachfragen zur DS-GVO nicht auffällig von der aus dem Jahr 2017 ab.

In der nachfolgenden Tabelle sind Angaben zur Anzahl der Eingaben und Beratungsanfragen dargestellt, die neben der Bearbeitung von Grundsatzfragen, Stellungnahmen zu Gesetzesvorhaben und der Marktbeobachtung im Bereich von IT-Produkten einen wesentlichen Teil meiner Tätigkeit ausmachen. Die Statistik wird weitgehend automationsgestützt mit Hilfe des eingesetzten Dokumentenverwaltungssystems erstellt. Die Anzahl der telefonischen Eingaben und Beratungen, die mehr als 10 Minuten in Anspruch nahmen, aber keinen Niederschlag in Akten fanden, wurden aus den Durchschnittsdaten des November 2017 fortgeschrieben, da keine signifikanten Abweichungen festgestellt werden konnten.

Die gegenüber dem Vorjahr etwas gestiegene Anzahl an schriftlich dokumentierten Beratungen in der ersten Jahreshälfte zeigte erste Anzeichen dafür, dass bereits einige für die Datenverarbeitung Verantwortliche im öffentlichen und nicht-öffentlichen Bereich die Brisanz der nahenden Rechtsänderungen erkannten.

Das tatsächliche Ausmaß wurde jedoch von vielen unterschätzt. Schlagartig änderte sich die Aufmerksamkeit mit dem 25.05.2018, dem Tag, an dem die DS-GVO Geltung erlangte.

(E= Eingabe/Beschwerde, B = Beratung)

Fachgebiet	**Anzahl 2017 gesamt (E+B)**	*Anzahl bis 24.05.2018 (E+B)*	*Anzahl ab 25.05.2018 (E+B)*	**Anzahl 2018 gesamt (E+B)**
Wohnen, Miete, Nachbarschaft	328	*148*	*248*	396
Auskunfteien und Inkassounternehmen	205	*118*	*533*	651
Schulen, Hochschulen, Archive	189	*78*	*296*	374
Elektronische Kommunikation, Internet	168	*120*	*414*	534
Beschäftigtendatenschutz	163	*59*	*197*	256
Kommunen	148	*52*	*172*	224
Adresshandel, Werbung	130	*71*	*161*	232
Gesundheit, Pflege	112	*142*	*397*	539
Kreditwirtschaft	102	*54*	*178*	232
Soziales	95	*40*	*62*	102
Polizei, Strafverfahren, Justiz, Verfassungsschutz	92	*104*	*153*	257
Verkehr	71	*39*	*134*	173
Handel, Handwerk, Gewerbe	67	*30*	*275*	305
IT-Sicherheit, DV-Technik und Herstelleranfragen	51	*30*	*54*	84
Betriebliche/Behördliche DSB	34	*4*	*468*	472
Versorgungsunternehmen	32	*48*	*76*	124
Vereine und Verbände	32	*16*	*323*	339
Versicherungen	27	*17*	*35*	52
Datenschutz außerhalb DE/EU	23	*0*	*5*	5
Rundfunk, Fernsehen, Presse	18	*4*	*21*	24
Forschung, Statistik	14	*10*	*4*	14
Steuerwesen	10	*4*	*7*	11
Ausländerrecht	10	*0*	*2*	2
Sonstige Themen < 10 (z. B. Religionen und Glaubensgemeinschaften, Landwirtschaft und Forsten, Geodaten)	68	*33*	*141*	174
Gesamtsumme dokumentierter Eingaben und Beratungen	**2.189**	***1.221***	***4.356***	***5.577***
davon Summe der dokumentierten Eingaben (ohne Abgaben)	2.001	*881*	*2.171*	3.052
davon Summe der dokumentierten Beratungen	188	*340*	*2.185*	2.525
davon Eingaben und Beratungen Videobeobachtung betreffend	260	*113*	*71*	184
zzgl. Summe telefonischer Beratungen	**5.808**	***2.420***	*nur Juni* ***1.703*** *Juli bis Dez.* ***3.036***	**7.159**
Gesamtsumme Eingaben und Beratungen	**7.997**	***3.641***	***9.095***	**12.736**

In einigen Bereichen stieg die Zahl der Eingaben (Beschwerden) sprungartig auf das Vielfache (Auskunfteien, elektr. Kommunikation, Handel usw.) an. In anderen Bereichen (Interne Datenschutzbeauftragte, Schulbereich, Kommunen, Vereine) war wiederum meine Beratung stärker gefragt. Im Nachhinein muss ich den Eindruck gewinnen, dass sich nur wenige Unternehmen, Vereine, Handel- und Gewerbetreibende etc. – aber auch öffentliche Stellen und Einrichtungen –, auch nur annähernd bewusst waren, welche Anforderungen die DS-GVO an sie stellen würde.

Die obige Übersicht stellt die Mengen bis 24.05.2018 dar.

3.6.2
Sanktionen

Im Berichtszeitraum wurden insgesamt 53 Ordnungswidrigkeitenverfahren, denen Verstöße gegen das BDSG a. F. zugrunde liegen, abgeschlossen. Damit konnte trotz der mit dem Wirksamwerden der DS-GVO verbundenen erheblichen Arbeitsbelastung ein Großteil der Rückstände aus den Vorjahren abschließend bearbeitet werden.

Insgesamt wurden elf Verfahren mit einem Bußgeldbescheid bzw. einer Verwarnung (§ 56 OWiG) beendet und Geldbußen bzw. Verwarnungsgelder in Höhe von 17.100 EUR festgesetzt. Vier Alt-Fälle konnten aus Kapazitätsgründen vor dem 25.05.2018 nicht mehr abschließend bearbeitet werden. Zwar unterfielen die Zuwiderhandlungen den Bußgeldtatbeständen des BDSG a. F., unter dem Regime der DS-GVO sind diese jedoch nicht mehr mit Geldbuße bedroht. In den betroffenen Fällen hatte die Änderung der Rechtslage zur Folge, dass das Tatzeitrecht (BDSG a. F.) aufgrund des in § 4 Abs. 3 OWiG normierten Prinzips der Meistbegünstigung nicht mehr angewendet werden konnte. Diese Ordnungswidrigkeitenverfahren mussten daher eingestellt werden.

Im Übrigen lagen den abgeschlossenen Verfahren vorwiegend Verstöße gegen die Tatbestände des § 43 Abs. 1 und Abs. 2 BDSG a. F. zugrunde. Es wurden Verstöße gegen die Auskunftspflicht gegenüber den Betroffenen oder der Aufsichtsbehörde sowie gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten geahndet. Weiterhin bezogen sich zahlreiche Verfahren auf Vorfälle im Zusammenhang mit einer unzulässigen Datenerhebung bzw. -verarbeitung. Außergewöhnliche Fälle gab es nicht.

3.6.3
Informationspflicht nach § 42a BDSG

Vom 01.01.2018 bis zum 24.05.2018 kam es zu 51 Meldungen nach § 42a BDSG alter Fassung. Davon waren 19 sogenannte Verdachtsfälle, die nach der damaligen Rechtslage nicht zu melden waren, und 32 begründete Meldungen.

Sachverhalt unrechtmäßiger Kenntniserlangung	Anzahl
Diebstahl von Kontounterlagen / Kundenunterlagen	3
Fehlerhafte Übermittlung von Kontodaten an Dritte	2
Fehlversand von Post mit Kontodaten	6
Fehlversand einer E-Mail mit personenbezogenen Daten diverser Kunden	1
Diebstahl von Laptops mit Kundendaten	1
Diebstahl Electronic-Cash Terminal	11
Fehlversand von Post mit personenbezogenen Daten gemäß § 3 Abs. 9 BDSG	3
Übermittlung personenbezogener Daten an unberechtigte Dritte	3
Fehlversand von Schreiben mit Gesundheitsdaten	2
Gesamtzahl der begründeten Meldungen	**32**

Zum Vergleich: Vom 25.05.2018 bis 31.12.2018 wurden 630 Datenschutzverletzungen nach Art. 33 DS-GVO gemeldet; siehe hierzu auch Ziff. 4.11.3 und 4.11.4.

4. Datenschutzbericht ab 25.05.2018 (nach DS-GVO, BDSG neu, HDSIG)

4.1 Querschnittthemen der DS-GVO

4.1.1 Zum Umfang des Auskunftsanspruchs nach Artikel 15 DS-GVO

Einen Anspruch auf Herausgabe einzelner Kopien – z. B. im Sinne einer Fotokopie bestimmter Dokumente – enthält Art. 15 Abs. *3 DS-GVO in aller Regel nicht: Die Pflicht, eine Kopie zur Verfügung zu stellen, ist nicht mit einem allgemeinem Recht auf Zugang zu Informationen oder einem Akteneinsichtsrecht gleichzusetzen.*

Gleichwohl können Verantwortliche im Einzelfall auch zur Übersendung einer Fotokopie eines bestimmten Dokuments verpflichtet sein. Dies kann dann der Fall sein, wenn das Recht der Betroffenen, die Rechtmäßigkeit der Datenverarbeitung eigenständig zu überprüfen, untrennbar hiermit verbunden ist.

Art. 15 DS-GVO

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- *a) die Verarbeitungszwecke;*
- *b) die Kategorien personenbezogener Daten, die verarbeitet werden;*
- *c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;*
- *d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;*
- *e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;*
- *f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;*
- *g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;*
- *h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.*

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 3 darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

In den letzten Monaten erreichten meine Behörde vermehrt Anfragen, die sich mit dem Auskunftsanspruch nach Art. 15 DS-GVO und insbesondere mit der Reichweite der Regelung des Art. 15 Abs. 3 DS-GVO beschäftigen.

Machen Betroffene ihr Auskunftsrecht nach Art. 15 DS-GVO geltend, so sind Verantwortliche gemäß Art. 15 Abs. 3 DS-GVO dazu verpflichtet, auch eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“, zur Verfügung zu stellen. Zu klären ist daher zum einen, ob Art. 15 Abs. 3 DS-GVO in Zusammenschau mit Art. 15 Abs. 4 DS-GVO ein eigenständiges, neben Art. 15 Abs. 1 DS-GVO stehendes Recht der betroffenen Person begründet. Zum anderen stellt sich die Frage der Interpretation – und damit letztlich der Reichweite – des Kopie-Begriffs.

Bedeutung des Auskunftsrechts

Das Auskunftsrecht des Art. 15 DS-GVO verfolgt in datenschutzrechtlicher Hinsicht verschiedene Ziele: Aus Erwägungsgrund 63 ergibt sich, dass Betroffene durch die Ausübung des Auskunftsrechts Bewusstsein über die Verarbeitung ihrer personenbezogenen Daten erlangen und in die Lage versetzt werden sollen, die Rechtmäßigkeit der Datenverarbeitung überprüfen zu können. Darüber hinaus kann Art. 15 DS-GVO den Weg für die Ausübung weiterer datenschutzrechtlicher Gestaltungsrechte, wie z. B. Recht auf Berichtigung gemäß Art. 16 DS-GVO oder Recht auf Löschung nach Art. 17 DS-GVO, bereiten oder der Geltendmachung von Schadensersatzansprüchen dienen.

Dem Auskunftsrecht kommt bei der Durchsetzung des Rechts auf informationelle Selbstbestimmung somit maßgebliche Bedeutung zu.

Umfang des Auskunftsrechts nach Art. 15 Abs. 1 DS-GVO

Der Bedeutung des Auskunftsrechts entsprechend legt Art. 15 Abs. 1 DS-GVO fest, dass die betroffene Person das Recht hat, von den Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Bejahen Verantwortliche die Verarbeitung personenbezogener Daten, so sind der betroffenen Person die in Art. 15 Abs. 1 lit. a bis h DS-GVO und Abs. 2 DS-GVO näher beschriebenen Informationen zur Verfügung zu stellen.

Keine Erweiterung des Auskunftsrechts nach Art. 15 Abs. 3 DS-GVO

Durch Art. 15 Abs. 3 DS-GVO werden Verantwortliche verpflichtet, „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", zur Verfügung zu stellen. Darüber hinaus spricht Art. 15 Abs. 4 DS-GVO vom „Recht auf Erhalt einer Kopie". Daher wird vertreten, dass es sich um eine inhaltliche Erweiterung im Sinne eines eigenständigen Herausgaberechts gegenüber dem in Art. 15 Abs. 1 DS-GVO enthaltenen Auskunftsrecht handelt.

Ich bin der Auffassung, dass Art. 15 Abs. 3 und 4 DS-GVO kein von Art. 15 Abs. 1 DS-GVO losgelöstes Recht ist. Verantwortliche müssen der in Art. 15 Abs. 3 DS-GVO enthaltenen Verpflichtung daher auch ohne entsprechenden Hinweis der Betroffenen nachkommen. Dafür spricht der Wortlaut des Art. 15 Abs. 3 DS-GVO. Hiernach ist Betroffenen eine Kopie der personenbezogenen Daten zur Verfügung zu stellen, die Gegenstand der Verarbeitung sind. Art. 15 Abs. 3 DS-GVO konkretisiert insofern den Wortlaut des Art. 15 Abs. 1 lit. b DS-GVO: Den Betroffenen sind nicht nur die Kategorien personenbezogener Daten, die verarbeitet werden, aufzuzeigen, sondern ihre spezifischen personenbezogenen Daten mitzuteilen. Art. 15 Abs. 3 DS-GVO präzisiert somit die in Art. 15 Abs. 1 lit. b DS-GVO enthaltene Regelung zum Umfang des Auskunftsrechts und bestimmt die Art und Weise (Kopie) der Auskunftserteilung.

Weitergehend ist zu beachten, dass der Europäische Gesetzgeber den Betroffenen nicht nur das in Art. 15 DS-GVO enthaltene Auskunftsrecht gewährt, sondern mit dem Recht auf Datenübertragbarkeit in Art. 20 DS-GVO einen eigenen Herausgabeanspruch zu Gunsten der Betroffenen begründet. Während das Auskunftsrecht den Betroffenen die Möglichkeit gibt, die Rechtmäßigkeit der Datenverarbeitung zu überprüfen, und diese damit gegebenenfalls erst in die Lage versetzt, weitergehende Datenschutzrechte (z. B. Berichtigung oder Löschung) geltend zu machen, soll es das Recht auf Datenübertragbarkeit den Betroffenen erleichtern, über ihre Daten zu verfügen (z. B. durch Verschieben in eine andere IT-Umgebung oder durch

Übertragung/Bereitstellung einer Kopie eines vorhandenen Datensatzes). Es ist daher nicht ersichtlich, warum Art. 15 Abs. 3, 4 DS-GVO ein neben Art. 20 DS-GVO stehendes Herausgaberecht begründen sollte.

Für den Inhalt des Auskunftsrechts gelten die allgemeinen Maßstäbe des Art. 12 DS-GVO. Die Auskünfte müssen präzise, transparent, verständlich und leicht zugänglich in einer klaren und einfachen Sprache formuliert sein. Das „Abspeisen" durch kommentarlose Überlassung von Kopien ist grundsätzlich nicht zulässig. Daraus folgt, dass Art. 15 Abs. 3 DS-GVO kein zusätzliches Recht auf Überlassung einer Kopie der personenbezogenen Daten meint, sondern voraussetzt, dass dem Auskunftsanspruch nach Art. 15 Abs. 1 DS-GVO die Überlassung einer Kopie ausreicht. Das Recht aus Art. 15 Abs. 4 DS-GVO reicht nicht weiter als die vorausgesetzten Rechte nach Art. 15 Abs. 1 und Abs. 3 DS-GVO.

Kein allgemeines Recht auf Zugang zu Informationen/ Akteneinsichtsrecht

Aufgrund des Wortlauts des Art. 15 Abs. 3 DS-GVO „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", stellt sich für Verantwortliche und Betroffene die Frage nach der Reichweite des Auskunftsrechts. Beschäftigt man sich mit der Bedeutung des Begriffs „Kopie", so findet man z. B. folgende Begriffsbeschreibungen: „Abschrift, Doppel eines Schriftstücks, Fotokopie, Nachahmung". Maßgeblich ist somit das Verständnis des in Art. 15 Abs. 3 DS-GVO verwendeten Kopie-Begriffs.

Wird in der „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind", das Doppel eines Schriftstücks oder eine Fotokopie verstanden (nachfolgend bezeichnet als „Kopie"), so würde dies dazu führen, dass Betroffene nach Art. 15 Abs. 3 DS-GVO z. B. einen generellen Anspruch auf die Übersendung sämtlicher geführter E-Mail-Korrespondenz hätten, sofern hierin Daten zu ihrer Person enthalten sind.

Ich verstehe den Kopie-Begriff des Art. 15 Abs. 3 DS-GVO im Sinne einer sinnvoll strukturierten Zusammenfassung. Den Betroffenen müssen daher nicht sämtliche, sie betreffende Dokumente in Kopie zur Verfügung gestellt werden.

Art. 15 Abs. 3 DS-GVO regelt lediglich die Art und Weise der Auskunftserteilung und hat gegenüber Art. 15 Abs. 1 DS-GVO dienende Funktion: Den Betroffenen wird noch einmal – durch Bereitstellung einer strukturierten Zusammenfassung ihrer personenbezogenen Daten – im Kontext kenntlich gemacht, welche Daten zu ihrer Person vom Verantwortlichen verarbeitet werden.

Dies entspricht auch der Wertung des Art. 12 Abs. 1 DS-GVO, wonach der Verantwortliche durch geeignete Maßnahmen alle Mitteilungen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln hat.

Art. 12 DS-GVO

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

(2) Der Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22. In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen.

(5) Informationen gemäß den Artikeln 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artikeln 15 bis 22 und Artikel 34 werden unentgeltlich zur Verfügung gestellt. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder

- *a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder*
- *b) sich weigern, aufgrund des Antrags tätig zu werden.*

Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.

…

Auch der Bedeutung des Auskunftsrechts ist hiermit vollumfänglich Rechnung getragen. Denn die Betroffenen werden hierdurch in die Lage versetzt, sich der Verarbeitung ihrer personenbezogenen Daten bewusst zu werden und die Rechtmäßigkeit der Datenverarbeitung zu überprüfen. Sie können ihre datenschutzrechtlichen Gestaltungsrechte ausüben und – sofern sie sich hierin verletzt sehen – z. B. Schadensersatzansprüche geltend machen oder ihr Recht auf Beschwerde bei einer Aufsichtsbehörde wahrnehmen.

Die Bereitstellung einer strukturierten Zusammenfassung entspricht auch dem Ziel der DS-GVO, natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu schützen, vgl. Art. 1 Abs. 1 DS-GVO. Wird der Kopie-Begriff des Art. 15 Abs. 3 DS-GVO grundsätzlich weit ausgelegt, so besteht die Gefahr, dass das Auskunftsrecht des Art. 15 DS-GVO als allgemeines Recht auf Zugang zu Informationen oder als Akteneinsichtsrecht verstanden wird, mit der Folge, dass die Geltendmachung von Art. 15 DS-GVO nicht zur Verfolgung von Datenschutzzielen im Sinne der DS-GVO, sondern zur Verwirklichung anderer Ziele missbraucht wird.

Schließlich entspricht das Verständnis des Begriffs als strukturierte Zusammenfassung auch der in Art. 15 Abs. 4 DS-GVO enthaltenen Wertung. Hiernach darf das Recht auf Erhalt einer Kopie gemäß Abs. 3 die Rechte und Freiheiten anderer Personen nicht beeinträchtigen. Werden den Betroffenen Kopien von Schriftstücken oder Dokumenten zur Verfügung gestellt, so kann sich bei mangelnder Sorgfalt das Risiko erhöhen, dass den Betroffenen auch Informationen zur Verfügung gestellt werden, die möglicherweise Rechte Dritter tangieren. Fertigen Verantwortliche hingegen eine strukturierte Zusammenfassung und tragen hierbei die personenbezogenen Daten der Betroffenen eigenständig zusammen, ist dieses Risiko deutlich minimiert.

4.1.2
Handhabung des Auskunftsrechts nach Art. 15 DS-GVO im Bereich des Beschäftigtendatenschutzes

Umfang sowie Art und Weise der Auskunftserteilung im Beschäftigungsverhältnis sind vom Verantwortlichen jeweils in einer Zusammenschau von Art. 15 Abs. 1 und Abs. 3 DS-GVO im Einzelfall zu bestimmen. Je nach Umständen kann die Auskunft durch eine strukturierte Zusammenfassung der Daten, die Gegenstand der Verarbeitung sind, oder einer Kopie erfolgen. Gehen Verantwortliche vom Vorliegen der Voraussetzungen einer Einschränkung des Auskunftsrechts aus, sind die Betroffenen hierüber zu informieren.

Durch ein Beschäftigungsverhältnis werden eine Vielzahl von personenbezogenen Datenverarbeitungen begründet. Mehrfach haben sich daher

Datenschutzbeauftragte und Verantwortliche an mich gewandt, wenn seitens Beschäftigter Auskunftsersuchen geltend gemacht wurden. Als Beispiele personenbezogener Datenverarbeitungen kommen die Führung der Personalakte oder die Nutzung eines Personalinformationssystems, die Durchführung von Personalentwicklungsmaßnahmen, Zeiterfassung oder Videoüberwachung in Betracht. Darüber hinaus emittieren Beschäftigte unter Berücksichtigung ihrer Tätigkeitsausübung Daten zu ihrer Person etwa bei der Nutzung der zur Verfügung gestellten IT-Infrastruktur (PC, Laptop, Mobiltelefon, Tablet) oder der geschäftlichen Kommunikation (Erstellung von Schriftstücken oder Kommunikation mittels E-Mail). Da das Arbeitsverhältnis naturgemäß auf eine gewisse Dauer angelegt ist, fallen diese Daten unter Umständen über Jahre und Jahrzehnte hinweg an.

Mit Blick auf Art. 15 DS-GVO empfehle ich Verantwortlichen und Datenschutzbeauftragten Folgendes:

Sofern Betroffene ihr Auskunftsrecht nach Art. 15 DS-GVO geltend machen, ist grundsätzlich losgelöst von der Ausübung des Rechts auf Erhalt einer Kopie nach Art. 15 Abs. 3 DS-GVO auch eine strukturierte Zusammenfassung der personenbezogenen Daten zur Verfügung zu stellen, die Gegenstand der Verarbeitung sind. Art. 15 Abs. 3 DS-GVO ergänzt und modifiziert das Auskunftsrecht des Art. 15 Abs. 1 DS-GVO und ist insbesondere vor dem Hintergrund des in Art. 5 Abs. 1 lit. a, 12 DS-GVO verankerten Transparenzgrundsatzes umzusetzen (siehe hierzu auch den Beitrag Ziff. 4.1.1).

Welche Vorgehensweise hierbei besonders geeignet erscheint, hängt von der zu beurteilenden Datenverarbeitung, mithin von den Umständen des Einzelfalls ab.

In den folgenden Konstellationen habe ich angenommen, dass den Anforderungen des Art. 15 Abs. 3 DS-GVO genüge getan ist:

– Bereitstellung eines Auszugs des Profils von Betroffenen bei Nutzung eines Personalinformationssystems durch Verantwortliche
– Liste der zu einer Person gespeicherten Schriftstücke oder Aktenzeichen bei Nutzung eines Dokumentenmanagement- oder Registratursystems

Sofern mit Verweis auf Art. 15 Abs. 3 DS-GVO die Kopie einzelner Schriftstücke oder E-Mail-Korrespondenzen verlangt wird, kann dieser Anspruch dann bestehen, wenn das Recht der Betroffenen, die Rechtmäßigkeit der Datenverarbeitung eigenständig zu überprüfen, untrennbar hiermit verbunden ist. Bei einer Zusammenschau von Art. 15 Abs. 1 und 3 DS-GVO und vor dem Hintergrund der Bedeutung des Auskunftsrechts dürfte es nach meinem Verständnis in aller Regel genügen, wenn den Betroffenen die in einem Schriftstück enthaltenen personenbezogenen Daten mitgeteilt werden.

Die Kopie eines Schriftstücks/einer E-Mail muss jedoch in der Regel nicht zur Verfügung gestellt werden.

Art. 15 Abs. 4 DS-GVO und Erwägungsgrund 63 sehen vor, dass das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen dürfen. Dies darf nach Erwägungsgrund 63 jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Auch Art. 23 DS-GVO ermöglicht Beschränkungen des Auskunftsrechts durch die Mitgliedstaaten. In Deutschland wurde von dieser Möglichkeit in den §§ 27 Abs. 2, 28 Abs. 2, 29 Abs. 1 Satz 2 und 34 BDSG Gebrauch gemacht.

Art. 23 DS-GVO

(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

a) die nationale Sicherheit;

b) die Landesverteidigung;

c) die öffentliche Sicherheit;

d) die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;

e) den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;

f) den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

g) die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;

h) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a, b, c, d, e und g genannten Zwecke verbunden sind;

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen;

j) die Durchsetzung zivilrechtlicher Ansprüche.

(2) Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf

a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien,
b) die Kategorien personenbezogener Daten,
c) den Umfang der vorgenommenen Beschränkungen,
d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung,
e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen,
f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien,
g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und
h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.

§ 34 BDSG

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach § 33 Absatz 1 Nummer 1, Nummer 2 Buchstabe b oder Absatz 3 nicht zu informieren ist, oder
2. die Daten
   a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder
   b) ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.

(3) Wird der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person

Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

Sofern Verantwortliche vom Vorliegen der Voraussetzungen einer Einschränkung des Auskunftsrechts ausgehen, sind die Betroffenen auch hierüber zu informieren. Dies ist sowohl Art. 12 Abs. 4 DS-GVO als auch § 34 Abs. 2 BDSG zu entnehmen. Denn nur auf Basis einer entsprechenden Information hat die betroffene Person die Möglichkeit, die Rechtmäßigkeit der Ablehnung des Auskunftsrechts zu überprüfen. Fehlen entsprechende Ausführungen des Verantwortlichen, ist dem Auskunftsrecht der betroffenen Person nicht Genüge getan.

Gemäß Art. 12 Abs. 5 DS-GVO ist die zu erteilende Auskunft unentgeltlich zur Verfügung zu stellen. Sofern Auskunftsersuchen allerdings offenkundig unbegründet (sehr selten) sind oder – insbesondere im Fall von häufiger Wiederholung – eine betroffene Person in exzessiver Weise Auskunftsanträge bei Verantwortlichen stellt, können diese ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Mitteilung berücksichtigt werden. Alternativ können sich Verantwortliche weigern, aufgrund des Auskunftsantrags tätig zu werden.

Gehen Verantwortliche davon aus, dass die Voraussetzungen des Art. 12 Abs. 5 DS-GVO erfüllt sind, haben sie die Betroffenen hierüber gemäß Art. 12 Abs. 4 DS-GVO zu informieren.

Zu beachten ist weiterhin, dass nach Art. 12 Abs. 5 DS-GVO Verantwortliche den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen haben. Die Verantwortlichen tragen somit die Beweislast.

Gemäß Erwägungsgrund 63 Satz 7 der DS-GVO können Verantwortliche verlangen, dass Betroffene ihr Auskunftsersuchen präzisieren, wenn eine große Menge von Informationen über die Betroffenen gespeichert wird. Dies ist bei Datenverarbeitungen im Beschäftigungsverhältnis anzunehmen, da hier, wie eingangs erwähnt, in großem Umfang und über einen langen Zeitraum personenbezogene Daten anfallen.

Vor dem Hintergrund der in tatsächlicher Hinsicht vielfältig anfallenden personenbezogenen Daten im Beschäftigungsverhältnis, dem Grundsatz der Transparenz (der in Art. 12 Abs. 1 DS-GVO insbesondere auch eine präzise, verständliche Form und eine klare und einfache Sprache fordert), dem Schutz von Rechten Dritter, der Unentgeltlichkeit des Auskunftsersuchens, der in Art. 12 Abs. 5 DS-GVO vorgesehenen Möglichkeit der Missbrauchsabwehr durch die Verantwortlichen und dem Präzisierungsgedanken des Erwägungs-

grund 63 DS-GVO sollten bei der Geltendmachung von Auskunftsersuchen im Beschäftigungsverhältnis folgende Gesichtspunkte beachtet werden:

– Den Betroffenen werden die Informationen nach Art. 15 Abs. 1 lit. a bis h DS-GVO zur Verfügung gestellt.
– Den Betroffenen werden (nach Wahl des Verantwortlichen und insbesondere vor dem Hintergrund der Schaffung von Transparenz nach Art. 12 DS-GVO) strukturierte Zusammenfassungen (z. B. Registraturauszug) oder Kopien zu allen Datenverarbeitungsvorgängen zur Verfügung gestellt, die zu ihrer Person verarbeitet werden.
– Werden strukturierte Zusammenfassungen oder Kopien mit Verweis auf bestehende Rechte Dritter abgelehnt, ist der betroffenen Person dies transparent mitzuteilen. Dies gilt auch für anderweitige Einschränkungen des Auskunftsrechts.
– Sofern personenbezogene Daten der Betroffenen in Datenverarbeitungen gespeichert sind, die nicht der Verarbeitung von Beschäftigtendaten dienen, sondern anderen Zwecken (z. B. Verarbeitung von Kundendaten) und somit nicht in Bezug auf den Anspruchssteller verarbeitet werden, genügt es, wenn Verantwortliche die Informationen nach Art. 15 Abs. 1 lit. a bis h DS-GVO zur Verfügung stellen und den Betroffenen die Möglichkeit einräumen, eine Präzisierung ihres Auskunftsersuchens vorzunehmen.

4.1.3
Pflicht zur Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

Aufgrund der Europäischen Datenschutzreform sind hessische Verantwortliche und Auftragsverarbeiter seit 25.05.2018 gemäß Art. 37 Abs. 7 DS-GVO verpflichtet, die Kontaktdaten der oder des Datenschutzbeauftragten dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit mitzuteilen. Verstöße gegen die Mitteilungspflicht an die zuständige Aufsichtsbehörde können mit einem Bußgeld geahndet werden.

Zur Abwicklung der Meldepflicht hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) ein Online-Meldeverfahren eingeführt, das unter https://datenschutz.hessen.de/service/benennung-eines-datenschutzbeauftragten zu erreichen ist. Die Implementierung des Online-Meldeformulars erfolgte am 14.05.2018. Seitdem sind im Berichtszeitraum ca. 15.000 Meldungen von 13.470 Stellen eingegangen.

Neben allen öffentlichen Stellen, die gemäß Art. 37 Abs. 1a, 4 DS-GVO i. V. m. § 5 Abs. 1 HDSIG das Amt des Datenschutzbeauftragten sowie des Stellver-

treters besetzen müssen und die benannten Personen über das Meldeportal zu melden haben, sind auch weitere Verantwortliche und Auftragsverarbeiter zur Benennung und Meldung einer oder eines Datenschutzbeauftragten verpflichtet. Neben den Voraussetzungen des Art. 37 Abs. 1 DS-GVO haben Verantwortliche und Auftragsverarbeiter die Regelungen des § 38 Abs. 1 BDSG zu berücksichtigen. Danach haben Verantwortliche und Auftragsverarbeiter eine oder einen Datenschutzbeauftragten zu benennen, wenn mindestens zehn Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Trotz der hohen Zahl an bereits eingegangenen Meldungen fällt immer wieder auf, dass eine Vielzahl von Verantwortlichen, Auftragsverarbeitern und auch öffentlichen Stellen in Hessen ihrer Verpflichtung zur Meldung noch nicht nachgekommen ist. Dieses Versäumnis ist umgehend zu beseitigen. Der HBDI überprüft im Rahmen der Bearbeitung von Vorgängen regelmäßig auch, ob der Pflicht zur Meldung nachgekommen wurde. Wenn nicht, wird dieser Umstand im Rahmen der Entscheidung über notwendige Maßnahmen mitberücksichtigt und kann daher auch zur Verhängung von Bußgeldern führen (siehe hierzu auch Ziff. 4.11.2).

4.1.4
Quittierung von Informationen nach Art. 13 und Art. 14 DS-GVO

Die Pflicht des Verantwortlichen, den Betroffenen über die Datenverarbeitung zu informieren, führt nicht zu einer Verpflichtung des Betroffenen, den Erhalt der Information durch Unterschrift zu quittieren.

Ein Bürger wandte sich an meine Dienststelle und beschwerte sich darüber, dass eine Kommune von ihm verlangte, den Erhalt der Information nach Art. 13 DS-GVO durch seine Unterschrift zu bestätigen. Weder Art. 13 noch Art. 14 DS-GVO sehen eine derartige Bestätigung durch den Empfänger der Information vor. Die Kommune stellte sich auf den Standpunkt, dass sie nur durch die Unterschrift des Empfängers ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachkommen könne.

> *Art. 5 Abs. 2 DS-GVO*
> *Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).*

M. E. fällt die Informationspflicht nach Art. 13/Art. 14 DS-GVO nicht unter die nach Art. 5 Abs. 1 DS-GVO nachzuweisenden Pflichten des Verantwortlichen.

Es ist demnach ausreichend, wenn der Verantwortliche dokumentiert, dass die Betroffenen gemäß Art. 13 und 14 DS-GVO informiert wurden. Weiterhin werden auch die häufig im Internet zur Verfügung gestellten Informationen dies belegen.

Eine vergleichbare Fragestellung im Bereich der Patienteninformation habe ich entsprechend bewertet (siehe Ziff. 4.6.1 und 4.6.2).

4.1.5
Aufzeichnung von Telefongesprächen (Call Recording) nach der DS-GVO

Das Aufzeichnen von Telefongesprächen (sog. Call Recording) ist zulässig, wenn die Betroffenen eine wirksame Einwilligung erteilt haben, es sei denn, es gibt gesetzliche Aufzeichnungs- und Aufbewahrungspflichten.

Ich erhielt einen Hinweis, dass bei einem Energiedienstleister für Heiz- und Betriebskostenabrechnungen standardmäßig Telefongespräche mit der Hotline aufgenommen werden. Eine ausdrückliche Einwilligung (Opt-in) seitens des Gesprächspartners wurde nicht eingeholt. Es erfolgte lediglich der Hinweis, dass der Gesprächspartner zu Beginn des Gesprächs einer Aufzeichnung widersprechen könne.

Mit Beschluss vom 23.03.2018 (Beschluss der DSK vom 23.03.2018 Aufzeichnung von Telefongesprächen; s. a. Materialien, Ziff. 2.3) haben die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) festgelegt, dass eine Aufzeichnung von Telefongesprächen datenschutzrechtlich in aller Regel nur mit Einwilligung auch des externen Gesprächspartners zulässig ist. Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO setzt demnach voraus, dass der Betroffene vor Beginn der beabsichtigten Aufzeichnung gefragt wird, ob er mit der Aufzeichnung einverstanden ist. Die Aufzeichnung bedarf der ausdrücklichen Zustimmung durch den Betroffenen bspw. durch das Aussprechen eines „Ja“ oder durch eine aktiv bestätigende Handlung (etwa durch das Betätigen einer Telefontaste). Ebenso muss die Einwilligung „in informierter Weise“ abgegeben werden. Das bedeutet, dass dem Gesprächspartner, bevor er die Einwilligung freiwillig erteilt, Informationen wie die Zwecke, die Speicherdauer etc. mitzuteilen sind.

Die Datenschutzkonferenz betont in ihrem Beschluss, dass die bloße Einräumung einer Widerspruchsmöglichkeit und das anschließende Fortsetzen des Telefonats keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO darstellt.

Der Energiedienstleister wurde daher von mir aufgefordert, das Verfahren der Telefonaufzeichnungen an die gesetzlichen Vorgaben anzupassen. Bis eine DS-GVO-konforme Lösung vorliegt, wurde das „Call Recording“ vorläufig komplett eingestellt.

4.1.6
Videoüberwachung durch Arbeitgeber

Arbeitgeber sind grundsätzlich berechtigt, öffentlich zugängliche Verkaufsräume durch Videokameras zu überwachen. Zur Rechtfertigung einer Videoüberwachung im Beschäftigtenkontext muss ein konkreter Anhaltspunkt zur Aufdeckung einer Straftat vorliegen. Unter Druck unterzeichnete Einwilligungserklärungen zur Videoüberwachung sind unwirksam.

Die Unsicherheit, wie die Videoüberwachung nach der Änderung des Bundesdatenschutzgesetzes sowie der Einführung der Datenschutzgrundverordnung im Mai 2018 rechtskonform eingesetzt werden kann, ist sowohl bei Privatpersonen als auch bei Gewerbetreibenden groß. So erreichten mich einerseits eine Reihe von telefonischen Anfragen und Schreiben zur Rückversicherung, dass die bisherige Videoinstallation gesetzeskonform sei. Andererseits wollten künftige Kamerabetreiber wissen, was sie vor einer Neu-Installation zu beachten hätten.

Zahlreiche Beratungsanfragen und Beschwerden wurden in diesem Jahr durch Arbeitnehmerinnen und Arbeitnehmer an mich gerichtet, deren Gegenstand die Videoüberwachung durch den eigenen Arbeitgeber war. So beschäftigte ich mich mit Fällen aus den Bereichen Gastronomie, Hotellerie, aber auch mit Gewerbetreibenden bis hin zu Seniorenpflegediensten.

So beschwerten sich in einem Fall gleich zwei Mitarbeitende eines Online-Großhandels (mit insgesamt 25 Mitarbeiter/-innen) unabhängig voneinander bei mir, dass eine Videoüberwachung sowohl im Büro (Großraumbüro) als auch im Lager sowie im Außenbereich des Firmengeländes stattfinden würde. Bildmaterial, das mir zur Verfügung gestellt wurde, belegte, dass durch Dome-Kameras mehrere Arbeitsbereiche und Schreibtische im Großraumbüro eingesehen werden konnten.

Das Firmengelände war umzäunt, der Zugang zu den Öffnungszeiten jedoch uneingeschränkt und jedermann möglich. Obwohl es sich um einen Online-Handel handelte, wurde angegeben, dass häufig Verkäufe vor Ort stattfänden und Kunden Waren besichtigten und kauften. Zu diesem Zweck war in einer Ecke des Großraumbüros ein Warentisch positioniert, um Produkte zu präsentieren. Die Einzelpreise der Produkte auf dem Tisch lagen

zwischen einem kleinen einstelligen Euro-Betrag bis zu ca. 500 EUR. Um vor einem Diebstahl der präsentierten Waren abzuschrecken oder gegebenenfalls einen Diebstahl zu ahnden, waren eine Dome-Kamera und eine Stabkamera im Großraumbüro installiert. Als weiterer Zweck der Überwachung wurde angegeben, dass bereits häufiger Diebstähle stattgefunden hätten. Zu Strafanzeigen sei es jedoch nicht gekommen.

Der Winkel der Aufnahme der Dome-Kamera konnte durch die schwarze Glaskuppel nicht eingesehen werden. Die Stabkamera war auf Schreibtische und einen Safe innerhalb des Großraumbüros ausgerichtet. Die Überwachung des Lagerraumes und des Außengeländes erfolgte durch Stabkameras.

Auf die Videoüberwachung wurde am Eingang des Gebäudes sowie im Lagerbereich mittels Piktogramm hingewiesen.

Rechtliche Bewertung

Die Videoüberwachung im öffentlichen Raum, also den kundenfrequentierten Bereichen, ist nach § 4 BDSG (Videoüberwachung öffentlich zugänglicher Räume) i. V. m. Art. 6 Abs. 1 lit. f DS-GVO (Rechtmäßigkeit der Verarbeitung) zu beurteilen.

Arbeitgeber sind nach dem Datenschutzrecht grundsätzlich dazu berechtigt, öffentlich zugängliche Verkaufsräume durch Videokameras zu überwachen, um sich vor Straftaten zu schützen, z. B. vor Diebstahl oder Vandalismus. Der Verkaufsbereich sowie der Bereich der Warenpräsentation waren hiervon umfasst.

Dabei muss der Zweck einer solchen Videoüberwachung nicht ausschließlich darin bestehen, Straftaten von Kunden abzuwehren. Vielmehr kann der Arbeitgeber daneben auch den Zweck verfolgen, sich vor Straftaten seiner Mitarbeiter zu schützen. Derartige Videokontrollen gibt es häufig in den Kassenbereichen von Einzelhandelsgeschäften. In solchen Fällen muss die Videoüberwachung offengelegt bzw. erkennbar gemacht werden, was üblicherweise durch Hinweisschilder und eine eindeutige Kameraausrichtung geschieht. Auf diese Weise können Kunden und Arbeitnehmer wissen, dass sie gefilmt werden. Außerdem muss der Arbeitgeber bzw. Ladeninhaber das Filmmaterial möglichst rasch wieder löschen.

Der übrige überwachte Bereich, in dem sich ausschließlich Beschäftigte aufhielten, ist nach Maßgabe des § 26 BDSG (Datenschutz für Zwecke des Beschäftigungsverhältnisses) zu bewerten.

Die Videoüberwachung zur Aufdeckung von Straftaten im Beschäftigtenkontext war schon deshalb unzulässig, weil kein konkreter Anhaltspunkt

oder Verdacht gegen einen oder mehrere Mitarbeiter/-innen vorlag, den es aufzuklären galt. Eine Begründung zur Überwachung der Büroarbeitsplätze konnte nicht erbracht werden.

Die Einwilligungserklärung, die der Arbeitgeber von seinen Mitarbeitenden eingeholt hatte und die diese unter Druck zu unterzeichnen hatten, wurde als unwirksam betrachtet, da es hier an der Freiwilligkeit fehlte. Eine Einwilligung innerhalb von Arbeitsverhältnissen ist nach § 26 Abs. 2 BDSG nur ausnahmsweise möglich, insbesondere, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Dies war hier nicht der Fall.

Ergebnis

Der Online-Handel wurde vor Ort geprüft. Zum Termin waren neben der Geschäftsführung der betriebliche Datenschutzbeauftragte und ein rechtlicher Vertreter anwesend. Jede Kamera wurde geprüft. Es konnte festgestellt werden, dass bereits Änderungen zu jener Situation vorgenommen wurden, die bei der Nachweisführung durch die Beschwerdeführer dargestellt wurde. In der Zwischenzeit wurden von den Mitarbeitenden unterzeichnete Einwilligungserklärungen zur Videoüberwachung am Arbeitsplatz eingeholt und mir vorgelegt, jedoch aus Mangel an der Freiwilligkeit der Unterzeichnung als unwirksam eingestuft.

Darüber hinaus wurden im Nachgang folgende Maßnahmen durchgeführt:

– Die Kamera, die direkt auf die Büroarbeitsplätze ausgerichtet war, wurde entfernt.
– Bei der übrigen Überwachung wurden sogenannte „private Zonen“ eingerichtet, bzw. bestehende Zonen wurden erweitert, damit keine Arbeitsplätze von der kontinuierlichen Überwachung betroffen sind.
– Das Großraumbüro wurde baulich umgestaltet. So wurde eine Spiegelwand, durch die Arbeitsplätze weitreichend eingesehen werden konnten, entfernt.
– Die Hinweisbeschilderung wurde um den Namen und die Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, den Zweck der Verarbeitung, die berechtigten Interessen sowie die Speicherdauer erweitert.
– Darüber hinaus wurde ein Großbildschirm im Großraumbüro installiert, der den Überwachungsmonitor einer jeden Kamera abbildete und damit eine umfängliche Transparenz garantierte.

Die Kameras im Lagerraum waren ausschließlich auf den Lagergang und das Zuliefertor gerichtet und nicht zu beanstanden.

Die Kameras im Außenbereich waren datenschutzkonform lediglich auf das eigene Grundstück ausgerichtet.

Auch wenn die Kamerainstallationen und das Überwachungssystem durch mich geprüft wurden und die Videoüberwachung im Unternehmen künftig mit der größtmöglichen Transparenz erfolgt, schien das Vertrauensverhältnis innerhalb der Belegschaft nachhaltig zerrüttet. Beide Beschwerdeführer arbeiten inzwischen nicht mehr im Unternehmen.

4.1.7
Bildaufnahmen und DS-GVO – keineswegs unmöglich

Ein Dauerbrenner unter den in meiner Behörde eingehenden Beschwerden sind solche über die Veröffentlichung von Bildern, vor allem im Internet. Zudem wurden im Berichtszeitraum unzählige Beratungsanfragen zur Aufnahme und Veröffentlichung von Fotos und Videos an mich herangetragen. Da die Rechtslage diesbezüglich seit der Datenschutzreform leider wenig eindeutig ist, herrscht bei vielen Verantwortlichen Unsicherheit, welche Bedingungen nun für die Aufnahme und Veröffentlichung von Bildern von Personen gelten.

Über den gesamten Berichtszeitraum hinweg erreichten mich dutzende schriftliche und telefonische Anfragen zu der Frage, unter welchen Bedingungen die Anfertigung und Veröffentlichung von Fotos und Videos nach dem neuen Datenschutzrecht zulässig ist. Die Anfragen stammten teilweise von Berufsfotografen, vor allem aber von Unternehmen, Privatpersonen und Vereinen, die zu verschiedenen Zwecken Fotos und Videos auf ihren Webseiten, Blogs und in Unternehmens- bzw. Vereinszeitschriften veröffentlichen wollten. In dieser Frage herrschte offensichtlich große Unsicherheit, die sicherlich nicht zuletzt durch inhaltlich teilweise fragwürdige Veröffentlichungen und lebhafte Diskussionen in Internetforen und sozialen Netzwerken angefacht wurde. Nicht selten wurde sogar die Befürchtung bzw. Wut darüber geäußert, dass aufgrund der DS-GVO nun vermeintlich gar keine Fotos mehr aufgenommen oder veröffentlicht werden dürften, wenn die abgebildeten Personen nicht ausdrücklich und schriftlich darin eingewilligt hätten. Dies ist natürlich nicht der Fall.

Digital aufgenommene Fotos und Videos, auf denen einzelne Personen erkenn- und identifizierbar sind, enthalten personenbezogene Daten. Das Fotografieren bzw. Filmen (Datenerhebung) und die Veröffentlichung der Bilder (Datenverarbeitung) fallen daher unter den Anwendungsbereich der DS-GVO. Genauso wie nach altem Recht sind jedoch zwei Fälle (weitgehend) vom Datenschutzrecht ausgenommen: Für die Fotografie zu rein persönlichen und familiären Zwecken (z. B. Urlaubsfotos) gilt das Datenschutzrecht

nicht, solange die privat aufgenommenen Fotos und Videos nicht in einem größeren Kreis veröffentlicht werden (z. B. Internet, Vereinszeitschrift). Eine weitere Ausnahme gilt für die Aufnahme und Veröffentlichung von Bildern und Videos zu journalistischen Zwecken (z. B. in Zeitungen, Fernsehen, professionellen Blogs etc.). Wie auch vor der Datenschutzreform gilt in diesem Bereich ausschließlich das Kunsturhebergesetz (KUG), dessen Anwendung die DS-GVO ausnahmsweise zulässt. In allen anderen Fällen gelten seit Mai 2018 für die Aufnahme und Veröffentlichung von Fotos und Videos ausschließlich die Regeln der DS-GVO. Alle nicht journalistisch tätigen Verantwortlichen (z. B. Vereine, Unternehmen, Webseitenbetreiber etc.) müssen sich beim Umgang mit Fotos und Videos daher nun nach den Anforderungen der DS-GVO richten.

Die Aufnahme und Veröffentlichung von Bildern ist danach problemlos zulässig, wenn die abgebildeten Personen darin eingewilligt haben (Art. 6 Abs. 1 S. 1 lit. a DS-GVO). Für die Einwilligungen gelten die Anforderungen aus Art. 4 Nr. 11 und Art. 7 DS-GVO. Sie müssen danach nicht unbedingt formell oder schriftlich erteilt werden, sondern können auch mündlich oder sogar konkludent, also beispielsweise durch Posieren vor der Kamera, erklärt werden. Allerdings trifft den Verantwortlichen im Zweifel eine Nachweispflicht. Zudem sind erteilte Einwilligungen jederzeit widerruflich und der Verantwortliche muss den Betroffenen vor Einholung der Einwilligung über deren Umfang und die Widerruflichkeit informieren.

Die DS-GVO sieht aber auch Möglichkeiten vor, Bilder und Videos ohne ausdrückliche Zustimmung der Abgebildeten aufzunehmen und zu veröffentlichen. So dürfen (Berufs-) Fotografen gemäß Art. 6 Abs. 1 lit. b DS-GVO im Rahmen ihres Auftrags Bilder von ihren Vertragspartnern aufnehmen und verarbeiten (z. B. Bewerbungsfotos, Hochzeitsfotos etc.). In den meisten Fällen ist aber anhand einer Interessensabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu beurteilen, ob das Anfertigen von Fotos und Videos bzw. deren Veröffentlichung zulässig ist oder nicht. Danach muss abgewogen werden zwischen einerseits den Interessen des Fotografen bzw. der Stelle, die die Bilder nutzen möchte, und andererseits den Rechten und Interessen der abgebildeten Person(en). In aller Regel hat die Person oder Stelle, die die Bilder aufnehmen bzw. veröffentlichen möchte, legitime Interessen daran, beispielsweise aus künstlerischen Gründen oder weil sie diese für ihre geschäftliche Tätigkeit benötigt oder für ihre Außendarstellung nutzen möchte. Die abgebildeten Personen haben dagegen ein generelles Interesse, nicht ohne ihr Wissen oder gegen ihren Willen abgebildet oder einem größeren Publikum präsentiert zu werden. Dieses Interesse ist allein durch die Aufnahme von Fotos oder Videos in der Öffentlichkeit regelmäßig nur geringfügig betroffen. Die Veröffentlichung oder Verbreitung der aufgenommenen Bilder

beeinträchtigt die Rechte und Interessen der Betroffenen dagegen sehr viel mehr. Je stärker die Rechte und Interessen der abgebildeten Personen durch die Bilder beeinträchtigt werden (z. B. detaillierte Porträtfotos, Fotos in brisanten Situationen/Posen) und je schutzbedürftiger diese sind (z. B. Kinder, hilflose Personen), desto eher ist die Veröffentlichung von Bildern und ggf. sogar bereits deren Aufnahme unzulässig. Die Interessenabwägung fällt allerdings immer dann zugunsten des Verantwortlichen aus, wenn die Veröffentlichung des jeweiligen Bildes auch nach den bereits nach alter Rechtslage angewandten Regeln des KUG zulässig wäre (insbesondere § 23 KUG). In diesen Fällen dürfen Bilder auch weiterhin ohne Einwilligung der Abgebildeten angefertigt und veröffentlicht werden.

Alle Personen, die auf Fotos und Videos abgebildet werden, müssen grundsätzlich nach Art. 13 bzw. 14 DS-GVO über die Hintergründe der Erhebung und Verarbeitung ihrer Daten informiert werden. Die Erfüllung der gesetzlichen Informationspflichten ist in der Praxis jedoch oft schwierig, da die im Bild festgehaltenen Situationen häufig flüchtig sind und zwischen Fotograf und Betroffenem oft keine verbale Kommunikation stattfindet und kein Medium eingesetzt wird, über das die Informationen einfach zugänglich gemacht werden könnten. Wenn mehrere Personen gleichzeitig fotografiert oder gefilmt werden und diesen teilweise gar nicht bewusst ist, dass sie aufgenommen werden (z. B. bei größeren Veranstaltungen oder Aufnahmen in Innenstädten), ist es regelmäßig unverhältnismäßig aufwendig oder sogar unmöglich und daher gemäß Art. 14 Abs. 5 lit. b DS-GVO auch entbehrlich, Informationen zum Datenschutz zu erteilen. Solchen Betroffenen, die wissen, dass sie abgebildet werden, muss der Verantwortliche hingegen die Informationen nach Art. 13 DS-GVO erteilen. Dies kann beispielsweise durch die Übergabe von Handzetteln oder durch den sichtbaren Aushang der Informationen an einem Veranstaltungsort (ggf. in Zusammenarbeit mit dem Veranstalter) geschehen.

Letztlich gelten für die Aufnahme und Veröffentlichung von Fotos und Videos von Personen auch nach der Datenschutzreform weitgehend die gleichen Anforderungen wie nach bisherigem Recht. Keinerlei Änderungen gibt es bei der Anfertigung und Veröffentlichung von Bildern zu rein privaten sowie zu journalistischen Zwecken. Auch in den übrigen Fällen sind die Anforderungen der DS-GVO lediglich in einigen wenigen Punkten (z. B. Einwilligung, Informationspflichten) etwas strenger als die des bisher maßgeblichen KUG.

4.2
Europa, Internationales

4.2.1
Internationale Datentransfers – Privacy Shield erneut auf dem Prüfstand

Auch in diesem Jahr war eine Mitarbeiterin des HBDI Mitglied der Delegation europäischer Aufsichtsbehörden, die gemeinsam mit der Europäischen Kommission und dem US-Handelsministerium sowie weiteren US-Behörden die praktische Umsetzung der zwischen der Europäischen Kommission und der US-Regierung ausgehandelten Bedingungen für einen Transfer von personenbezogenen Daten aus der EU in die USA unter dem EU-US-Privacy Shield geprüft hat.

Im Berichtsjahr fand die Überprüfung in Brüssel statt. Die etwa 40-köpfige Delegation aus den USA wurde von Handelsminister Wilbur Ross angeführt. Die europäische Delegation, angeführt von Kommissarin Jourová, setzte sich aus sieben Vertretern der europäischen Datenschutz-Aufsichtsbehörden und Vertretern der Europäischen Kommission zusammen.

Wie schon bei der Überprüfung im letzten Jahr (46. Tätigkeitsbericht, Ziff. 4.1, S. 55 ff.) umfasste die Prüfung zunächst Fragen nach der praktischen Umsetzung des Privacy Shield. Hier lag der Fokus vor allem auf Ablauf und Inhalt des (Re-)Zertifizierungsprozesses und den Mechanismen, mit denen sichergestellt werden soll, dass die zertifizierten Unternehmen die Bedingungen auch tatsächlich erfüllen und zum Beispiel gewährleisten, dass Betroffene die ihnen nach dem Privacy Shield zustehenden Rechte auch tatsächlich ausüben können.

Seinen Bericht zur zweiten jährlichen Überprüfung des Privacy Shield hat der Europäische Datenschutzausschuss (EDSA) unter https://edpb.europa.eu/our-work-tools/our-documents/other/eu-us-privacy-shield-second-annual-joint-review-report-22012019_en veröffentlicht. Es konnte insgesamt festgestellt werden, dass die Prozesse, die auf Seiten des US-Handelsministeriums und der Federal Trade Commission ergriffen wurden, in die richtige Richtung weisen. Die Schlussfolgerungen, die die Artikel 29-Datenschutzgruppe in ihrem Bericht zur ersten Überprüfung des EU-US-Privacy Shield für diesen Bereich gezogen hatte, wurden sämtlich angenommen und es wurde daran gearbeitet, die praktische Umsetzung in diesem Sinne weiter zu verbessern.

Im diesjährigen Bericht werden jedoch auch Bereiche benannt, in denen weitere Arbeit nötig ist: Größter Kritikpunkt bleibt die Sorge, dass die Aufsicht über die zertifizierten Organisationen eher auf formale Aspekte beschränkt sein könnte und zu wenig substanzielle Kontrollen stattfinden. Ein weiterer

Punkt, der im kommenden Jahr näher betrachtet werden sollte, sind die Weiterübermittlungen von Privacy Shield-zertifizierten Unternehmen an Dritte. Hier muss aus Sicht des EDSA sichergestellt werden, dass die im Privacy Shield hierzu festgelegten Bedingungen in der Realität auch eingehalten werden. Schließlich sollen auch weiterhin der Bereich der Beschäftigtendaten und der Rezertifizierungsprozess im Auge behalten werden.

Neben den praktischen Umsetzungsfragen nahm auch wieder die Frage nach staatlichen Zugriffen auf Daten, die unter dem Privacy Shield in die USA transferiert wurden, einen großen Raum ein. Auch hier kann festgehalten werden, dass einige Schlussfolgerungen der Artikel 29-Datenschutzgruppe aus dem vergangenen Jahr von den US-Behörden aufgegriffen wurden. So wurden kurz vor der zweiten jährlichen Überprüfung des Privacy Shield ausreichend viele neue Mitglieder für den Privacy and Civil Liberties Oversight Board benannt, um das Gremium wieder beschlussfähig zu machen.

Allerdings ist auch festzuhalten, dass die Position der Ombudsperson, die eigens mit dem Privacy Shield geschaffen wurde, um eine Möglichkeit für Betroffene zu eröffnen, ihre Rechte bei staatlichen Zugriffen auf personenbezogene Daten wirksam durchzusetzen, nach wie vor nur interimsweise besetzt ist. Die Europäische Kommission hat dies dazu veranlasst, den USA in ihren Schlussfolgerungen zur zweiten Überprüfung des Privacy Shield ein Ultimatum zu setzen. Sollten die USA bis zum 28.02.2019 keinen Kandidaten für das Amt der Ombudsperson nominiert haben, kündigt die Europäische Kommission an, „angemessene Maßnahmen nach der Datenschutz-Grundverordnung“ zu ergreifen. Eine mögliche Maßnahme wäre danach auch die Aussetzung des Privacy Shield. Der Bericht der Europäischen Kommission ist unter https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf abrufbar.

Insgesamt kann erneut festgestellt werden, dass das Gebiet der internationalen Datentransfers weiterhin mit gravierenden Unsicherheiten belastet ist. Neben der indirekten Drohung der Europäischen Kommission, den Privacy Shield aufzuheben, sind weiterhin Verfahren vor dem EuGH anhängig, deren Ausgang weitreichende Bedeutung für die Zulässigkeit von Datentransfers in Staaten außerhalb der EU haben wird.

4.2.2
Europaweite Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden nach der Datenschutz-Grundverordnung

Durch die Datenschutz-Grundverordnung (DS-GVO) ergeben sich für die Zusammenarbeit der Aufsichtsbehörden in Deutschland und Europa zahlreiche Neuerungen. Die beim HBDI neu eingerichtete Stabsstelle Europa und Internationales fungiert als Bindeglied für die Kommunikation zwischen dem HBDI und verschiedenen Stellen außerhalb Hessens in Deutschland, Europa und der Welt.

Die DS-GVO zwingt die einzelnen Aufsichtsbehörden zu einer viel engeren Zusammenarbeit als bisher. Sie verfolgt konsequent den Gedanken des One-Stop-Shop. Das bedeutet, dass ein Unternehmen, das ein Datenverarbeitungsverfahren über Niederlassungen in mehreren Mitgliedstaaten hinweg einsetzt oder das bei nur einer Niederlassung ein Verfahren einsetzt, das aber erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat, sich nur mit einer Aufsichtsbehörde (federführende Aufsichtsbehörde) auseinandersetzen müssen soll.

Der One-Stop-Shop gilt jedoch auch auf Seiten der Betroffenen: Diese haben die Möglichkeit, sich mit einer Beschwerde an eine beliebige Aufsichtsbehörde (die dadurch zur betroffenen Aufsichtsbehörde im Sinne von Art. 4 Nr. 22 DS-GVO wird) in Europa zu wenden. Die Kommunikation mit dem Betroffenen ist dann allein dieser Aufsichtsbehörde zugewiesen, auch wenn sie für die Stelle, gegen die sich die Beschwerde richtet, nicht zuständig ist.

Daraus folgt, dass zumindest Beschwerden gegen Stellen außerhalb Deutschlands vom HBDI nicht mehr an die für die Stelle, gegen die sich die Beschwerde richtet, „zuständige“ Aufsichtsbehörde abgegeben werden dürfen. Es ist nun vielmehr so, dass derlei Fälle zwischen dem HBDI und der oder den anderen betroffenen Aufsichtsbehörden kommuniziert und gemeinsam bearbeitet werden müssen.

Ziel der neuen Verfahrensregelungen ist es, eine möglichst europaweit einheitliche Auslegung und Anwendung der DS-GVO sicherzustellen. Darüber hinaus soll die Kommunikation mit den Aufsichtsbehörden sowohl für datenverarbeitende Stellen als auch für betroffene Personen vereinfacht werden.

Die Verfahrensweisen, die hier zur Anwendung kommen, sind im Wesentlichen in Kapitel VII der DS-GVO geregelt. Um die geforderte Zusammenarbeit auch elektronisch zu ermöglichen und zu erleichtern, wird unter anderem IMI (Internal Market Information System, deutsch: Binnenmarkt-Informationssystem) eingesetzt. Seit dem 25.05.2018 waren vom HBDI im Berichtszeitraum bereits über 400 in IMI eingetragene Fälle mit steigender Tendenz in der

neuen Form der europäischen Zusammenarbeit zu bearbeiten. Fast alle dieser Fälle wären dem HBDI vor der Geltung der DS-GVO entweder gar nicht zur Kenntnis gelangt oder direkt an die „zuständige“ Aufsichtsbehörde verwiesen worden, in deren Aufsichtsbereich die Stelle, gegen die sich die Beschwerde richtet, ihren Sitz hat.

Ein zusätzliches Novum für die Arbeit des HBDI in Fällen, die nach der DS-GVO nun mit anderen Aufsichtsbehörden in Europa bearbeitet und abgestimmt werden müssen, ist die fast ausschließliche Englischsprachigkeit der Arbeit.

Die DS-GVO stellt also nicht nur für datenverarbeitende Stellen und Betroffene eine Herausforderung dar, sondern bedeutet auch für den HBDI und die anderen deutschen und europäischen Datenschutzaufsichtsbehörden einen erheblichen kommunikativen und organisatorischen Mehraufwand, der zu bewältigen ist.

4.3
Allgemeine Verwaltung, Kommunen, Polizei

4.3.1
Projekt „Digitale Modellbehörde“

Die Hessische Landesverwaltung hat 2018 das Projekt „Digitale Modellbehörde“ begonnen. Ziel ist es, eine Vielzahl von Verwaltungsleistungen zu digitalisieren. Der HBDI begleitet das Projekt im Lenkungsausschuss und, soweit erforderlich, auch in den Teilprojekten.

Das OZG als rechtlicher Rahmen

Das Onlinezugangsgesetz (OZG) ist ein Bundesgesetz, das seit dem 18.08.2017 in Kraft ist. Es verpflichtet Bund und Länder (gemäß Begründung und Intention des Bundes einschließlich der Kommunen), innerhalb von fünf Jahren ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten.

Wesentliche Zielvorgaben des OZG sind

– die zügige Digitalisierung des Online-Zugangs zu Verwaltungsleistungen bis 2022,
– die Verknüpfung einzelner Verwaltungsportale zu einem Portalverbund und
– die Bereitstellung von interoperablen Nutzerkonten für einen einheitlichen, komfortablen und sicheren Zugang zu online angebotenen Verwaltungsleistungen, unabhängig davon, ob auf kommunaler, Landes- oder Bundesebene.

Das Projekt „Digitale Modellbehörde“

Mit dem Projekt „Digitale Modellbehörde“ soll am Beispiel der drei Regierungspräsidien die Umwandlung von Behörden in digitale Servicedienstleister in Gang gesetzt werden. Es geht im Wesentlichen um die Digitalisierung des Online-Zugangs und der internen Verwaltungsabläufe. Dabei sollen die Abläufe medienbruchfrei sein und eine schnellere, effizientere und wirtschaftlichere Bearbeitung gewährleisten. Es gilt aber auch, die Kommunen in die Abläufe einzubinden.

Die Projektstruktur sieht einen Lenkungsausschuss für die Projektsteuerung vor. Dem Lenkungsausschuss gehöre ich als beratendes Mitglied an. Unter dem Lenkungsausschuss befindet sich die Projektleitung, worunter wiederum Teilprojekte und Unterstützungsleistungen firmieren.

In einem ersten Schritt wurden fünf fachliche Teilprojekte (TP) gestartet. Zum Teilprojekt „Anerkennungsprämie“ siehe auch mein Beitrag unter Ziff. 4.3.2.

Außerdem gab es noch Teilprojekte, die insbesondere dazu dienten, Ist-Zustände zu erfassen und übergreifende Aspekte zu systematisieren.

Der Aspekt Datenschutz

Aus meiner Sicht war es wesentlich sicherzustellen, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Dazu gab es mehrere Gespräche mit der Projektleitung. Im Ergebnis wurde eine Struktur gefunden, die die wesentlichen datenschutzrechtlichen Prüfungen und Freigaben in den Teilprojekten belässt, wobei es im koordinierenden Querschnittsbereich (als Share Service bezeichnet) einen Koordinator gibt, der für Rückfragen zur Verfügung steht.

Der Standardprozess sieht an einer Reihe von Stellen vor, die Einhaltung datenschutzrechtlicher Vorgaben sicherzustellen:

– Während der Initiierung wird das Verzeichnis der Verarbeitungstätigkeiten durch den Verantwortlichen erstellt.
– Am Ende der Phase wird u. a. entschieden, ob eine Datenschutzfolgenabschätzung durchgeführt werden muss.
– Im folgenden Umsetzungsplan müssen insbesondere die Anforderungen des Art. 25 DS-GVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy by design“ und „Privacy by default“) beachtet werden.
– Am Ende des Umsetzungsplans wird geprüft, ob die datenschutzrechtlichen Annahmen weiterhin gültig sind. Wenn nicht, sind entsprechende Anpassungen vorzunehmen.

– In der anschließenden Umsetzung können sich Änderungen ergeben. Diese sind mit dem Querschnittsbereich abzuklären. Danach wird die Stellungnahme des zuständigen Datenschutzbeauftragten angefragt, um bei positiver Stellungnahme das Pilotprojekt zu starten.
– Am Ende des Pilotprojekts werden die Erfahrungen ausgewertet und es ergeben sich eventuell Änderungen. Bei relevanten Änderungen erfolgt wieder eine Rücksprache mit dem Querschnittsbereich. Es wird wieder geprüft, ob die Vorgaben des Datenschutzes weiterhin eingehalten werden. Ist das der Fall, erfolgt die Überführung in den Regelbetrieb.

Wenn die Teilprojekte nach diesen Vorgaben durchgeführt werden, kann die Einhaltung der Anforderungen aus der DS-GVO und dem HDSIG angenommen werden.

4.3.2
„Digitale Modellbehörde“ – Teilprojekt „Anerkennungsprämie“

„Anerkennungsprämie“ ist ein Teilprojekt der „Digitalen Modellbehörde“. Es geht dabei darum, die Gewährung von Prämien für Mitglieder freiwilliger Feuerwehren zu digitalisieren. Dabei sind Kommunen, ihre Feuerwehren und auch Regierungspräsidien involviert.

Worum es geht

Seit 2011 erhalten ehrenamtliche Feuerwehrangehörige in Einsatzabteilungen und seit 2017 ehrenamtliche Helferinnen und Helfer in den Einheiten des hessischen Katastrophenschutzes eine Anerkennungsprämie für eine aktive Dienstzeit von 10, 20, 30 oder 40 Jahren.

Die Anträge werden von den Kommunen und in den Fällen des Katastrophenschutzes durch die Landkreise oder kreisfreien Städte an das Land Hessen gestellt. Das jeweils zuständige Regierungspräsidium bearbeitet die Anträge. Im bisherigen Ablauf erreichten die Anträge in Papierform die Präsidien, wo sie für die weitere Bearbeitung in Excel-Tabellen übernommen wurden.

In dem Projekt „Digitale Modellbehörde“ wurde die Beantragung und Auszahlung dieser Anerkennungsprämien als eine Verwaltungsleistung identifiziert, bei der eine Digitalisierung schnell erfolgen kann und zu einer wesentlichen Beschleunigung und auch Verbesserung führt (siehe dazu auch den Beitrag unter Ziff. 4.3.1).

Das Teilprojekt „Anerkennungsprämie“

Für das Teilprojekt haben Mitarbeiterinnen und Mitarbeiter der Regierungspräsidien zusammen mit Vertretern der ekom21 die Vorgaben für eine webbasierte Datenbankanwendung erarbeitet. Als Basis diente die eGovernment-Plattform „civento“. Zusammen mit Vertretern des HMDIS wurden die entsprechenden Dokumente erstellt und mir präsentiert. Eine Schwellwertanalyse kam zu dem Ergebnis, dass keine DSFA erforderlich ist; das Ergebnis war für mich nachvollziehbar. Auch wurde der Erlass überarbeitet und eine Vereinbarung nach Art. 26 DS-GVO getroffen.

Schwierig war es, die Verhinderung von doppelten Vergaben einer Anerkennungsprämie im Prozess datenschutzgerecht zu gestalten. Gleiches galt, wenn jemand keine Anerkennungsprämie erhalten wollte, obwohl sie ihm nach dem Erlass zugestanden hätte. Hier musste auf § 28a HDSIG zurückgegriffen werden, um eine datenschutzgerechte Lösung zu erhalten.

Die geplante Lösung

Die Anträge können grundsätzlich nur elektronisch gestellt werden. Für die elektronische Antragstellung stellt das Land Hessen den Gemeinden und Landkreisen bzw. kreisfreien Städten kostenlos ein entsprechendes IT-System (civento-Anerkennungsprämie) zur Verfügung.

Das IT-System besteht aus einem Online-Teil für die Antragstellung. Die Gemeinden und Landkreise bzw. kreisfreien Städte können die Datenerfassung für die Antragstellung an die Einheiten der freiwilligen Feuerwehr oder des Katastrophenschutzes delegieren. Um sicherzustellen, dass nur die jeweils berechtigten Organisationen via Online-Portal die Antragstellung vorbereiten, erhalten diese Organisationen entsprechende Zugänge mittels User-ID und Passwort. Alternativ können die Gemeinden und Landkreise bzw. kreisfreien Städte die Antragstellerdaten mittels eines Erfassungstools im System direkt erfassen.

Nach der Erfassung der Daten der zu Ehrenden durch die berechtigten Organisationen überprüfen die Gemeinden und Landkreise bzw. kreisfreien Städte diese Angaben und stellen den Antrag auf Anerkennungsprämie beim zuständigen Regierungspräsidium. Die Daten werden elektronisch an die Regierungspräsidien übermittelt.

Zum Zwecke der Antragstellung werden folgende Daten erhoben:

<u>Von der Antragstellerin/vom Antragsteller:</u>

– Name
– Vertretungsberechtigter

– Anschrift
– E-Mail-Adresse
– Telefonnummer
– geplanter Verleihungstermin

Die Angaben werden aufgrund der gespeicherten Nutzerdaten vorgesteuert.

Von der/dem zu Ehrenden:

– Familienname
– Vorname
– Geburtsdatum
– Geschlecht
– Wohnort: Straße
– Wohnort: Hausnummer
– Wohnort: Zusatz zur Hausnummer/Buchstabe
– E-Mail-Adresse
– Dienstzeiten

Wird der Antrag gestellt, so wird der Datensatz an das zuständige Regierungspräsidium übermittelt.

Wird der Antrag abgelehnt, so muss dazu eine Begründung gegeben werden. In diesem Fall erfolgt keine Übermittlung der Daten an die Regierungspräsidien. Die Begründung der Ablehnung ist nur für interne Zwecke des Antragstellers vorgesehen.

Wurde die Urkunde übergeben, werden darüber hinaus die Daten durch die Gemeinden oder Landkreise erweitert und den Regierungspräsidien übermittelt:

– Übergabe der Urkunde zum geplanten Zeitpunkt
– Übergabe der Urkunde „Datum“ wenn vom geplanten Zeitpunkt abweichend
– keine Übergabe der Urkunde und Hinderungsgründe

Mit der Übergabe der Urkunde erhalten die zu Ehrenden neben dem persönlichen Anschreiben der Regierungspräsidentin bzw. des Regierungspräsidenten ein weiteres Schreiben. Dieses Schreiben enthält die Zugangsdaten (PIN) für das civento-Portal. Die Geehrten können dort ihre Bankdaten erfassen:

– IBAN
– BIC
– ggf. abweichende/r Kontoinhaber/-in

Alternativ können die Antragsteller oder die Regierungspräsidien diese Angaben erfassen.

Nach der Erfassung der Daten der zu Ehrenden überprüfen die Gemeinden und Landkreise diese Angaben und stellen den Antrag mittels Datenübermittlung an die Regierungspräsidien. Das Regierungspräsidium prüft unabhängig die Angaben erneut und erstellt – bei Vorliegen der Voraussetzungen – eine Urkunde, ein Anschreiben der Regierungspräsidentin oder des Regierungspräsidenten und ein Anschreiben mit der Bitte, die Kontodaten via Online-Portal zu erfassen. Die Unterlagen werden den Antragsstellern auf dem Postweg zugestellt. Wird eine Anerkennungsprämie abgelehnt, informiert das Regierungspräsidium die Gemeinden und Landkreise unter Angabe der Ablehnungsgründe.

Nach der Verleihung der Urkunden und der Übergabe der Anschreiben an die Geehrten übermitteln die Gemeinden und Landkreise die Angaben an die Regierungspräsidien. Die Regierungspräsidien veranlassen nach der Erfassung der Kontodaten (im Online-Portal entweder durch die Geehrten oder durch die Gemeinden und Landkreise) die Auszahlung der Anerkennungsprämie durch das Erstellen einer entsprechenden Auszahlungsanordnung. Soll die Erfassung der Kontodaten auf Bitten der Geehrten durch die Gemeinden oder Landkreise erfolgen, kann dies nur im Rahmen des Online-Portals erfolgen. Hierfür müssen die Geehrten die Zugangsdaten aus dem Anschreiben bekannt geben. Die Regierungspräsidien können die Kontodaten im Rahmen der Vorgangsbearbeitung direkt im Vorgang erfassen.

Die Daten der Gemeinden und Landkreise werden mit Ablauf des auf die Ehrung folgenden Jahres gelöscht. Die Daten der Regierungspräsidien werden nach Ablauf des zehnten auf die Verleihung folgenden Jahres gelöscht. Eine Übergabe der Daten und Dokumente in das System der dauerhaften Langzeitspeicherung des Landes Hessen wird vorgesehen. Hierfür werden im Rahmen eines weiteren Teilprojekts des Digitalisierungsprogramms sowohl die technischen als auch organisatorischen Voraussetzungen geschaffen.

4.3.3
Veröffentlichungen auf kommunalen Internetseiten

Zahlreiche Anfragen von Kommunen sowie Beschwerden kommunaler Bediensteter, aber auch von Bürgerinnen und Bürgern betreffen die Veröffentlichungen auf kommunalen Internetseiten. Hierzu finden sich bereits Ausführungen in meinem 43. Tätigkeitsbericht.

Die Kommunen verfolgen mit Veröffentlichungen unterschiedliche Zwecke. Es geht darum, Transparenz zu erzeugen, Mitwirkung zu ermöglichen und Bürgerinnen und Bürger zu informieren. Inwieweit es hierzu der Veröffentlichung von unmittelbar personenbezogenen Daten oder auch von Daten, die

einen Personenbezug erlauben, bedarf, ist im Einzelfall zu prüfen. Dabei sind Erforderlichkeit und Verhältnismäßigkeit einer Veröffentlichung auch nach der Reichweite des genutzten Mediums und damit der Tiefe des Eingriffs in das Recht auf informationelle Selbstbestimmung zu beurteilen.

In der Regel werden veröffentlichte Sachverhalte einer Kommune nur für einen begrenzten Personenkreis, beispielsweise für deren Bürgerinnen und Bürger der Kommune, von Belang sein. Eine derartige Adressatenbegrenzung ist bei Veröffentlichung auf kommunalen Internetseiten nicht möglich. Personenbezogene Sachverhalte werden dort einer weltweiten Öffentlichkeit zugänglich gemacht und ermöglichen auch entsprechende und erfolgreiche Suchanfragen, ohne dass ein globales Erfordernis zur Kenntnisnahme vorliegt. Das Informationsinteresse der Internetöffentlichkeit an personenbeziehbaren Informationen über Bürgerinnen und Bürger hat dabei gegenüber den Interessen der von der Veröffentlichung Betroffenen zurückzutreten.

Daraus ergibt sich, dass eine, letztlich weltweite, Veröffentlichung personenbezogener Daten nur in begründeten Einzelfällen über kommunale Internetseiten erfolgen darf. In diesen Fällen ist der zur Verfügung gestellte Inhalt dahingehend zu begrenzen, dass sich die Information nur dem designierten Empfängerkreis erschließt. Beispielsweise ist die Veröffentlichung einer personellen Veränderung in einer wichtigen Position innerhalb einer Kommune auf Grundlage des § 66 Abs. 2 HGO darauf zu begrenzen, dass diese Position nun durch Person B und nicht mehr durch Person A wahrgenommen wird. Weitere Informationen zu den jeweiligen Personen oder den Gründen der Veränderungen dürfen in Ermangelung eines Erfordernisses nicht veröffentlicht werden.

4.3.4
Auskunft aus polizeilichen Auskunftssystemen des Landes Hessen

Durch die Neuregelungen der EU-Datenschutzreform wird den Bürgerinnen und Bürgern die Inanspruchnahme ihrer Auskunftsrechte erleichtert und auch den neuen Kommunikationswegen Rechnung getragen. Entsprechende Erleichterungen erfahren die Bürgerinnen und Bürger auch bei Inanspruchnahme ihrer Auskunftsrechte gegenüber der Hessischen Polizei.

Zuständig für die Beauskunftung aus dem polizeilichen Informationssystem POLAS-Hessen ist das Hessische Landeskriminalamt (HLKA).

Vor dem 25.05.2018 forderte dieses ein Anschreiben mit beigefügter, beglaubigter oder bestätigter Kopie eines Ausweispapieres sowie die Angabe einer Postanschrift der auskunftsersuchenden Person. Das Verlangen nach

einer Kopie hatte ich akzeptiert, da dies als zwingend angesehen wurde, um den Betroffenen eindeutig zu identifizieren und den Missbrauch zu vermeiden. Diese bisherige Vorgehensweise machte es den auskunftspflichtigen Stellen in der Vergangenheit damit recht einfach sicherzustellen, dass die Auskünfte von einer/einem Berechtigten gestellt wurden und auch nur an die/den Berechtigte/en gelangten.

Diese Praxis konnte unter der neuen Rechtslage so nicht aufrechterhalten werden. Die Rahmenbedingungen für die Auskunft aus den polizeilichen Auskunftssystemen ergeben sich nunmehr aus § 29 HSOG und § 54 HDSIG.

Aus § 54 Abs. 4 HDSIG ergibt sich, dass nur bei begründeten Zweifeln an der Identität zusätzliche Informationen von dem oder der Betroffenen gefordert werden dürfen. Demnach muss die auskunftspflichtige Stelle im Einzelfall prüfen, ob ein Auskunftsantrag sich aufgrund der vorliegenden Informationen zweifelsfrei einer bestimmten Person zuordnen lässt und dass die abschließende Auskunft der berechtigten Person übermittelt wird. Die auskunftspflichtige Stelle muss einen Grad der Gewissheit über die Identität des Antragstellers erlangen, der ein Auffinden in den betreffenden Datenbeständen ermöglicht und weiterhin eine zweifelsfrei an den Berechtigten gerichtete Beauskunftung zulässt. Zum Auffinden von Personen in polizeilichen Datenbeständen sind grundsätzlich Angaben zu Name/n, Vorname/n und Geburtsdatum erforderlich, zur Auskunftserteilung, die aus datenschutzrechtlichen Gründen grundsätzlich schriftlich auf den Postweg erfolgt, eine Postanschrift. Soweit sich eine Person, beispielsweise aufgrund von Mehrfachbeständen in einer Datei, nicht zweifelsfrei identifizieren lässt, dürfen die erforderlichen Informationen ergänzend beim Betroffenen angefordert werden, die eine Identifizierung ermöglichen. Begründete Zweifel an der Identität des Antragsstellers können auch durch teilweise, vom polizeilichen Datenbestand abweichende Informationen entstehen, oder auch, wenn eine genannte Absenderadresse dem Antragsteller nicht zugeordnet werden kann.

Das HLKA hat seine Praxis diesen Vorgaben angepasst. Nach meiner Kenntnis war bisher in nur einer äußerst geringen Anzahl von Anfragen das Einholen ergänzender Informationen bei der betroffenen Person notwendig.

4.3.5
Datenaustausch zwischen Industrie- und Handelskammern und der Finanzverwaltung

Die Industrie- und Handelskammern sind befugt, die zu Festsetzung der Kammerbeiträge erforderlichen Daten bei der Finanzverwaltung zu erheben.

Mehrfach wandten sich Gewerbetreibende mit der Frage an mich, ob die Finanzverwaltung befugt sei, den Industrie- und Handelskammern personenbezogene Daten betreffend die finanziellen (steuerlichen) Verhältnisse der Gewerbetreibenden zu übermitteln. Auslöser der Anfragen war zumeist, dass die Gewerbetreibenden von den Industrie- und Handelskammern wegen Mitgliedschaft und Beitragsfestsetzung angeschrieben worden waren.

§ 3 Abs. 2 IHKG regelt, dass die Kosten der Errichtung und Tätigkeit der Industrie- und Handelskammern u. a. durch Beiträge der Kammerzugehörigen gemäß einer Beitragsordnung aufgebracht werden. Kammerzugehörige sind neben Unternehmen auch natürliche Personen, sofern sie zur Gewerbesteuer veranlagt sind und im Bezirk der Industrie- und Handelskammer eine Betriebsstätte unterhalten (§ 2 Abs. 1 IHKG). Die Registergerichte übermitteln den Industrie- und Handelskammern die Eintragungen ins Handelsregister.

Datenschutzrechtlich sind die Industrie- und Handelskammern gemäß § 9 Abs. 2 IHKG (i. V. m. Art. 6 Abs. 1 lit. e DS-GVO) befugt, die zur Feststellung der Kammerzugehörigkeit erforderlichen Daten bei den Finanzbehörden zu erheben.

§ 9 Abs. 2 IHKG

Die Industrie und Handelskammern … sind berechtigt, zur Feststellung der Kammerzugehörigkeit und zur Festsetzung der Beiträge der Kammerzugehörigen Angaben zur Gewerbesteuerveranlagung … sowie die … erforderlichen Bemessungsgrundlagen bei den Finanzbehörden zu erheben.

Diese Erhebungsbefugnis der IHKs wird in der Abgabenordnung (§ 31) durch eine entsprechende Übermittlungspflicht der Finanzbehörden, die insbesondere auf die Industrie- und Handelskammern zielt, komplettiert.

§ 31 Abs. 1 AO

Die Finanzbehörden sind verpflichtet, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts … zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermessbeträge oder Steuerbeträge anknüpfen.

Über diese Rechtslage habe ich die Anfragenden informiert.

4.3.6
Anfertigung und Nutzung von 360°-Panoramaaufnahmen zur Berechnung wiederkehrender Straßenbeiträge

Das Anfertigen von 360°-Panoramaaufnahmen von Gebäuden und Straßen durch eine private Firma ist datenschutzrechtlich zulässig. Auch die Übermittlung solcher Aufnahmen an eine Gemeinde und deren Nutzung zur Berechnung wiederkehrender Straßenbeiträge zur Erfüllung einer öffentlichen Aufgabe ist nicht zu beanstanden.

Zu klären war, ob das Erstellen von 360°-Panoramaaufnahmen von Gebäuden und Straßen eines privaten Unternehmens sowie die Weiterleitung dieser Aufnahmen an eine Gemeinde, die diese zur Berechnung wiederkehrender Straßenbeiträge verwendet, datenschutzrechtlich zulässig sei.

Eine Gemeinde kaufte von einem privaten Anbieter 360°-Panoramaaufnahmen, um den Bestand der Straßen und Gebäude der Gemeinde zu ermitteln. Hierfür wurden die Straßen mit speziellen Fahrzeugen abgefahren, die mit Videokameras und einer entsprechenden Sensorik ausgestattet sind. Die durch die Videofahrzeuge erhobenen Daten geben Aufschluss über die Größe von Grundstücken, deren Bebauung (z. B. Wohn- oder gewerbliches Gebäude, ein- oder mehrgeschossig etc.) sowie über den Straßenzustand. Diese Daten können Aufschlüsse über sachliche Verhältnisse einer identifizierbaren Person geben und sind damit personenbezogene Daten. Die so erhobenen Daten nutzte die Gemeinde zur Berechnung wiederkehrender Straßenbeiträge.

Anfertigung und Übermittlung von Panoramaaufnahmen durch das Unternehmen

Die Verarbeitung personenbezogener Daten ist unter anderem zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist und schutzwürdige Interessen oder Grundrechte und Grundfreiheiten der Betroffenen nicht überwiegen (Art. 6 Abs. 1 lit. f DS-GVO). Dabei kann ein berechtigtes Interesse bereits ein ideelles oder wirtschaftliches Interesse des Verantwortlichen oder eines Dritten darstellen (vgl. Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 6 DS-GVO, Rdnr. 54).

Im vorliegenden Fall basiert das Geschäftskonzept des beauftragten Unternehmens darauf, für öffentliche und private Organisationen 360°-Panoramaaufnahmen von Gebäuden und Straßen zu fertigen und ihnen bereitzustellen. Seitens des Unternehmens ist daher ein geschäftliches und damit wirtschaftliches Interesse an der Verarbeitung der personenbezogenen Daten zu sehen. Die Rechtmäßigkeit ist jedoch davon abhängig, dass schutzwür-

dige Interessen der Betroffenen im Rahmen der von dem Verantwortlichen vorgenommenen Abwägung seine berechtigten Interessen nicht überwiegen.

Während der Befahrung werden auch in der Umgebung befindliche Fahrzeuge und deren Kennzeichen aufgezeichnet. Ferner werden auch Personen aufgezeichnet, die sich auf den Straßen aufhalten. Dies stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Aus diesem Grund werden durch das Unternehmen die aufgenommenen Personen und Kfz-Kennzeichen verpixelt und damit anonymisiert. Die Veröffentlichung von Panoramaaufnahmen findet nicht statt.

Zu beachten ist, dass das Widerspruchsrecht nach Art. 21 DS-GVO der betroffenen Person bei Vorliegen bestimmter Voraussetzungen das Recht einräumt, eine rechtmäßige und auf gesetzlicher Grundlage des Art. 6 Abs. 1 S. 1 lit. e und f DS-GVO erfolgende Verarbeitung sie betreffender personenbezogener Daten zu unterbinden. Das Widerspruchsrecht ist an das Vorliegen von Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben müssen, geknüpft. Es veranlasst sodann Verantwortliche zur Abwägung dieser konkret geltend gemachten Gründe mit den eigenen berechtigten Interessen an der Verarbeitung. Personenbezogene Daten von widersprechenden Personen dürfen nur dann verarbeitet werden, wenn zwingende schutzwürdige Gründe für die Verarbeitung nachgewiesen werden können, die die konkret geltend gemachten Gründe der betroffenen Person überwiegen.

Unter diesen Voraussetzungen ist die oben geschilderte Form der Erhebung und Übermittlung der Daten durch das beauftragte Unternehmen in Rahmen der Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO zulässig. Die besondere Situation der betroffenen Person ist im Rahmen der Abwägung des Art. 21 Abs. 1 S. 2 DS-GVO zu berücksichtigen.

Verwendung durch die Gemeinde zur Berechnung wiederkehrender Straßenbeiträge

Ferner prüfte ich, ob die Datenverarbeitung seitens der Gemeinde als Empfänger der Panoramabilder zulässig ist. Als Rechtsgrundlage für die Verarbeitung nach der Datenschutzgrundverordnung kam Art. 6 Abs. 1 lit. e DSG-VO in Betracht. Danach ist die Verarbeitung zulässig, wenn sie für die Wahrnehmung einer öffentlichen Aufgabe, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Gemäß § 93 Hessische Gemeindeordnung (HGO) i. V. m. § 11 Abs. 1 S. 2 Kommunales Abgabengesetzes (KAG) soll die Gemeinde für den Umbau und Ausbau der öffentlichen Straßen, Wege und Plätze (Verkehrsanlagen),

die über die laufende Unterhaltung und Instandsetzung hinausgeht, Beiträge erheben. Dabei räumt § 11a KAG ein Wahlrecht ein, diese auch über wiederkehrende Straßenbeiträge zu erheben. Die Unterhaltung von öffentlichen Straßen und die damit zusammenhängende Erhebung von Beiträgen stellt eine öffentliche Aufgabe in der Zuständigkeit der Gemeinde dar.

Der Betrag, den die Grundstückseigentümer in diesem Zusammenhang zu zahlen haben, setzt sich aus der Grundstücksgröße, der Nutzungsart, der Anzahl der Geschosse und dem Beitragssatz entsprechend des Abrechnungsgebiets zusammen. Die 360°-Panoramaaufnahmen der Gebäude und Straßen lieferten diese Daten, die schließlich zur Berechnung der wiederkehrenden Straßenbeiträge erforderlich waren. Diese Daten werden intern von der Gemeinde zu diesem Zweck genutzt.

Somit werden die Panoramabilder für die Beitragserhebung von Straßenbaumaßnahmen im Rahmen der Aufgabenerfüllung genutzt und sind damit datenschutzrechtlich zulässig.

4.4
Schule, Hochschulen

4.4.1
Keine WhatsApp im Schulalltag für Lehrkräfte – Gibt es eine Alternative?

Die Nutzung von WhatsApp im schulischen Bereich durch Lehrkräfte hat im Berichtsjahr stark zugenommen. Dabei wird die Handreichung des Kultusministeriums zur Nutzung von Sozialen Medien durch Lehrkräfte nicht ausreichend beachtet.

Der Messenger WhatsApp

WhatsApp ist ein sogenannter Instant-Messenger-Dienst, der es erlaubt, zwischen registrierten Nutzern Text- und Sprachnachrichten sowie Fotos, Videos, Audiodateien und Kontaktdaten auszutauschen und via IP-Telefonie über das Internet zu telefonieren. Nach eigenen Angaben hatte WhatsApp im Jahre 2016 eine Milliarde Nutzerinnen und Nutzer. Das tägliche Volumen der Kommunikation lag bei 42 Milliarden Nachrichten, 1,6 Milliarden Fotos und 250 Millionen Videos. WhatsApp ist damit der meistgenutzte Messenger-Dienst weltweit. Die Zahl der WhatsApp-Nutzer in Deutschland wird auf 32 Millionen Köpfe geschätzt. Im Oktober 2014 wurde WhatsApp von dem Sozialen Netzwerk Facebook übernommen.

Im Gegensatz zu Facebook, das mit Werbung auf Grundlage der Daten der Nutzerinnen und Nutzer seine Umsätze erzielt, war das Geschäftsmodell von

WhatsApp lange unklar. Die Zusicherung im Zusammenhang mit der Übernahme von WhatsApp durch Facebook, weiterhin unabhängig zu arbeiten und die Daten beider Dienste nicht miteinander zu vermischen, wurde von WhatsApp mit der Änderung seiner Nutzungsbedingungen Mitte des Jahres 2016 aufgehoben.

Welche Daten werden von WhatsApp gespeichert?

Daten, über die WhatsApp unter anderem verfügt, sind:

– Telefonnummer
– Profilname, Profilbild
– Nachrichten
– Gruppenzugehörigkeit
– Favoritenlisten
– Nutzungsinformationen
– Transaktionsdaten
– Geräte- und Verbindungsdaten
– Standortdaten
– Cookies
– Statusinformationen

Daraus lassen sich teils detaillierte Beziehungs-, Kommunikations-, Bewegungs-, Nutzungs- oder Interessenprofile bilden.

Die datenschutzrechtliche Problematik

Bei der Nutzung eines Messengers wie WhatsApp findet eine Verarbeitung von personenbezogenen Daten statt. Der Nutzer muss sich anmelden, Kommunikationsinhalte werden ausgetauscht, wobei auch sog. Verkehrsdaten entstehen. Zudem werden mit der Anmeldung automatisch alle im Mobiltelefon gespeicherten Kontakte an den Anbieter übertragen. Für diese Datenverarbeitungsprozesse ist entweder eine Rechtsgrundlage oder eine Einwilligung der Betroffenen erforderlich. Der Nutzer von WhatsApp ist für die Übermittlung der in seinem Mobiltelefon gespeicherten Kontaktdaten anderer Personen datenschutzrechtlich verantwortlich. Er muss daher vor Anmeldung des Messenger-Dienstes über die entsprechende Erlaubnis verfügen. Das Amtsgericht Bad Hersfeld hat im Beschluss vom 20.03.2017 (F 111/17 EASO) zu diesem Thema ausgeführt, dass, wer durch die Nutzung von WhatsApp die andauernde Weitergabe seiner Mobiltelefon-Kontakte zulässt, ohne vorher von seinen Kontaktpersonen eine Erlaubnis eingeholt zu haben, gegenüber diesen Personen eine deliktische Handlung begehe und sich in die Gefahr begebe, von diesen kostenpflichtig abgemahnt zu werden.

Ob und in welchem Umfang eine Lehrkraft in ihrem privaten Umfeld WhatsApp nutzt, ist zunächst einmal deren persönliche Sache. Wenn es aber um die Verarbeitung personenbezogener, schulischer Daten geht, befindet sich die Lehrkraft in einem anderen rechtlichen Kontext. Die Lehrkraft tritt im Namen der Schule auf, diese ist verantwortliche Stelle und muss grundsätzlich für die Sicherheit und Nachvollziehbarkeit der Datenverarbeitung und der Kommunikation garantieren. Nach § 83 des Hessischen Schulgesetzes (HSchG) ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist. Auch aus § 3 Abs. 5 der Verordnung zur Verarbeitung personenbezogener Daten in Schulen ergibt sich diese Verpflichtung für Schulen und damit auch für die Lehrkräfte. Erforderlichkeit setzt voraus, dass der Zweck nur mit dieser Datenverarbeitung erreicht werden kann. Eine bloße Erleichterung des Schulalltages kann die Erforderlichkeit nicht begründen. Somit liegt für die Nutzung von WhatsApp keine Rechtsgrundlage vor.

Auch von einer Einwilligung kann nicht ohne Weiteres ausgegangen werden. Zum einen verlangen die Nutzungsbedingungen von WhatsApp ein Mindestalter von 16 Jahren. Zum anderen ist eine Einwilligung nur wirksam, wenn sie freiwillig erteilt wurde. Eine solche Freiwilligkeit kann im schulischen Zusammenhang in der Regel kaum unterstellt werden.

Schließlich ist mit der Nutzung von WhatsApp auch eine Übermittlung der Daten außerhalb des Europäischen Wirtschaftsraums verbunden. Das Unternehmen hat seinen Sitz in Kalifornien/USA und müsste sich den datenschutzrechtlichen Vorgaben der Europäischen Union zum Datentransfer in die USA unterwerfen. Da die WhatsApp Inc. sich nicht dem Privacy Shield Abkommen unterworfen hat (siehe https://www.privacyshield.gov/list), ist die Übermittlung bereits nach den Vorgaben des Art. 44 DS-GVO unzulässig.

Alternativen zu WhatsApp

Immer wieder wird der Eindruck erweckt, es gäbe zu WhatsApp keine Alternativen. Die Stiftung Warentest z. B. hat bereits im Jahr 2015 Messenger-Dienste unter die Lupe genommen und Produkten wie Threema, Hoccer oder Signal datenschutzfreundliche Funktionalitäten attestiert. So stehen die Server in Deutschland (Hoccer), Threema (Schweiz) oder den USA (Signal). Auch der Dienst stash cat, den ich eingehender betrachtet habe, wäre eine akzeptable Alternative. Personenbezogene Daten werden nicht oder nur in geringem Umfang erhoben, Telefonbücher des Mobiltelefons nicht ausgelesen. Bei Hoccer zum Beispiel wird jedem Nutzer ein zufällig generierter

Zahlencode zur Verfügung gestellt, sozusagen als Benutzername. Freunde lassen sich über den Zahlencode hinzufügen oder über einen QR-Code. Auch eine Ende-zu-Ende-Verschlüsselung ist gewährleistet.

Es stellt sich also die Frage, warum Lehrkräfte, wenn diese schulisch mit ihrer Klasse kommunizieren möchten, nicht diese Dienste nutzen. Den Kultusminister habe ich im Rahmen eines Gesprächs im Juni vergangenen Jahres auch auf dieses Thema angesprochen. Dabei kam zum Ausdruck, dass er den Bedarf für einen datenschutzkonformen, landeseinheitlichen Messenger-Dienst für Schulen durchaus sieht. Allerdings steht das Ministerium noch am Anfang derartiger Überlegungen und nicht zuletzt gibt es auch finanzielle Zwänge, denen sich das HKM ausgesetzt sieht.

Unabhängig hiervon ist es jedoch unter den Vorgaben der DS-GVO für Schulen bzw. die Lehrkräfte zwingend, die Datenverarbeitung im Rahmen der Nutzung derartiger Dienste datenschutzgerecht zu organisieren.

4.4.2
Internetbasierte Lernverlaufsdiagnostik mit quop

Die hessenweite Einführung der Lernverlaufsdiagnostik-Software quop habe ich datenschutzrechtlich begleitet. Hinsichtlich der Erfordernisse, die sich aus der Datenschutz-Grundverordnung ergeben, mussten durch den Auftragsverarbeiter und das Hessische Kultusministerium eine Reihe von Vorgaben umgesetzt werden.

Was ist quop?

Die internetbasierte Lernverlaufsdiagnostik mit quop basiert auf einer Reihe von Erkenntnissen aus Forschung und Praxis. Das Verfahren quop erfasst die Leistungsentwicklung von Schülerinnen und Schülern in kurzen zeitlichen Abständen in den zentralen Leistungsbereichen Lesen (Klassenstufen 1 bis 6), Mathematik (Klassenstufen 1 bis 6) sowie Englisch (Klassenstufen 5 und 6) am Computer.

Die auf den Lernverlauf ausgerichtete Diagnostik verfolgt das Ziel, Lehrkräften eine verlässliche Informationsbasis zur individuellen Anpassung und Optimierung des Lernprozesses der Schüler während des Schuljahres bereitzustellen. Lehrkräfte erhalten dadurch fortlaufende Informationen über die tatsächlichen Kompetenzen einzelner Schülerinnen und Schüler und können darauf zielorientiert mit Einzelmaßnahmen für das Kind, z. B. einer Änderung von Umfang und Inhalt des Lehrinhaltes, reagieren.

Datenschutzrechtliche Aspekte

Auftragsverarbeitung

Bei dem Verfahren ist ein Auftragsverarbeiter eingeschaltet, der für das Hessische Kultusministerium (HKM) das Verfahren zentral betreibt. Mit diesem war ein Vertrag über eine Auftragsverarbeitung gemäß Art. 28 DS-GVO abzuschließen, da im Rahmen der Anwendung personenbezogene Daten der Schülerinnen und Schüler sowie der Lehrkräfte verarbeitet werden.

Welche personenbezogenen Daten werden erfasst?

Von den Lehrkräften werden systemisch Name, Vorname, E-Mail-Adresse, Klasse-Fach-Kombinationen und Telefonnummer gespeichert. Von den Schülerinnen und Schülern werden Name, Vorname, Passwort, zugeordnete Testreihe (Fach und Stufe), Geschlecht, Geburtstag, besonderer Förderbedarf (ja/nein), Migrationshintergrund (ja/nein) und Einschulungsjahr erfasst. Im Rahmen der automatisierten Auswertung nach der Bearbeitung von Testaufgaben werden Daten der Schülerinnen und Schüler hinsichtlich des Lernstandes in Lesen und/oder Mathematik und/oder Englisch ausgewiesen, die der Schülerin / dem Schüler selbst und der Lehrkraft zur Verfügung stehen.

Technische Datenschutz-Aspekte

Technik des Verfahrens

Computerbasierte Verfahren für die Schule müssen grundsätzlich für die dort vorhandenen Rahmenbedingungen geeignet sein. Schulcomputer haben in der Regel keine einheitlichen, technischen Standards und unterschiedliche Nutzungszeiträume. Auch werden teilweise alte Geräte mit uneinheitlichen Wartungs- und Sicherheitskonzepten genutzt sowie verschiedenste Betriebssysteme eingesetzt.

Sowohl den Lehrkräften als auch den Schüler/-innen wird quop als eine in einem Browser lauffähige Web-Anwendung über das Internet bereitgestellt. Dies hat den Vorteil, dass keine zusätzliche Installation von Software auf den Arbeitsplatzrechnern in den Schulen notwendig ist. Eine Anwendung im häuslichen Bereich der Schülerinnen und Schüler ist nicht vorgesehen. Zum anderen kann die Software auf der Plattform des Auftragsverarbeiters im Rahmen der immer wieder notwendigen Aktualisierungen zentral gepflegt werden.

Verschlüsselung

Die personenbezogenen Daten zwischen den Rechnern in der Schule und dem Server des Auftragsverarbeiters werden mit den aktuellen Verfahren

zur Transportverschlüsselung geschützt übertragen. Beim Auftragsverarbeiter sind die Daten pseudonymisiert abgelegt. Der Auftragsverarbeiter hat keinen Zugriff auf die Pseudonyme. Der Zugang zum Pseudonym (also die Verbindung zu Namen und einer Nummer, unter der die Daten abgespeichert sind) ist vielmehr an die Berechtigungen der jeweiligen Lehrkraft gebunden.

Zugang zur Anwendung

Der Zugang zum Portal ist passwortgeschützt. Das Erstpasswort wird den Schulen über das HKM postalisch zugestellt und ist ein Schulpasswort. Die Lehrkraft meldet sich mittels des Schulpasswortes auf dem Portal an, vervollständigt das eigene Benutzerkonto (Registrierung) und kann danach mit einem individuellen Benutzerkonto/Passwort mit der Anwendung arbeiten. Die Lehrkraft kann nun innerhalb der Anwendung ihre Klasse einrichten und für die Schülerinnen und Schüler die notwendigen individuellen Passwörter anlegen.

Freischaltung von zusätzlichen Lehrkräften

Die „federführende“ Lehrkraft kann in erforderlichem Umfang für weitere Lehrkräfte den Zugang zu den Lernstandserhebungen in Form von Leseberechtigungen freischalten und diese auch wieder entziehen. Dies steht im Zusammenhang mit einem zusätzlichen und erweiterten Beratungsbedarf durch z. B. Vertretungskräfte, die einerseits im Bedarfsfall klassische Vertretungsfunktionen abdecken und über den Lernstand der Schülerinnen und Schüler Informationen benötigen, wie auch ggf. einem konkreten Beratungsbedarf unter den Lehrkräften selbst, die mit den Kindern in Kontakt sind. Die federführende Lehrkraft sorgt dann auch wieder dafür, dass die Zugriffe, sofern nicht mehr erforderlich, entzogen werden.

Löschung der Daten

Wechselt die verantwortliche Lehrkraft die Klasse oder verlässt die Schule, so werden alle Berechtigungen entzogen. Verlässt ein Schüler bzw. eine Schülerin die Klasse oder wechselt die Schule, so werden die personenbezogenen bzw. personenbeziehbaren Daten zum Ende des jeweiligen Schuljahres hin gelöscht. Die gleiche Löschfrist gilt, soweit quop im Unterricht nicht mehr zum Einsatz kommen sollte. Im Übrigen bleiben die Daten so lange gespeichert, bis die Schülerin bzw. der Schüler die Jahrgangsstufe 6 abgeschlossen hat.

Mandantentrennung

Der Softwareanbieter hat in der bisher angebotenen Form des Verfahrens die Trennung der Daten für die Schulen verschiedener Bundesländer nur an einzelnen Merkmalen des Datenbestands vorgenommen. Damit wird das Verfahren den Anforderungen, die an einen landesweiten Einsatz zu stellen sind, nicht gerecht. Damit die unterschiedlichen vertraglichen Anforderungen der beauftragenden Länder und ggf. einzelner Schulen auch unabhängig voneinander umgesetzt werden können, ist eine verbesserte Mandantentrennung, z. B. durch eine kundenspezifische Virtualisierung, geboten. Ich habe das Hessische Kultusministerium darauf aufmerksam gemacht, dass eine Umsetzung dieser technischen Forderung durch den Auftragsverarbeiter für eine datenschutzgerechte Umsetzung unverzichtbar ist.

Datenschutzrechtliche Zulässigkeit

Nach dem Hessischen Schulgesetz dürfen personenbezogenen Daten von den Schulen verarbeitet werden.

§ 83 Abs. 1 HSchG

Schulen dürfen personenbezogene Daten von Schülerinnen und Schülern, deren Eltern und Lehrerinnen und Lehrer verarbeiten, soweit dies zur rechtmäßigen Erfüllung des Bildungs- und Erziehungsauftrages der Schule und für einen jeweils damit verbundenen Zweck oder zur Durchführung schulorganisatorischer Maßnahmen erforderlich ist.

Ein Ausführungserlass des HKM beschreibt und regelt den Umgang mit quop im Einzelnen. So werden darin Umfang und Nutzung der Lernstandsdiagnostik geregelt. Nach einer Information in der Gesamtkonferenz und der Zustimmung der Schulleitung kann sich die jeweilige Lehrkraft für die Nutzung von quop beim Hessischen Kultusministerium anmelden. Über ein Registrierungsverfahren erhält die Lehrkraft dann den Zugang zu einem persönlichen Nutzerkonto. Weitere Hinweise im Erlass betreffen Zugangsrechte und Löschfristen.

Zusammen mit dem Erlass ist das Verfahren auf eine rechtlich fundierte Basis gestellt, der einheitliche Maßstäbe zugrunde liegen.

4.4.3
„Schule ohne Rassismus – Schule mit Courage“ – auch ein begrüßenswertes Projekt hat den Datenschutz zu beachten

Das Verfahren zur Erlangung der Auszeichnung „Schule ohne Rassismus – Schule mit Courage“ ist mit den aktuellen datenschutzrechtlichen Bestimmungen nicht vereinbar und daher datenschutzkonform anzupassen.

Anlässlich der Beratungsanfrage einer hessischen Schule zu dem oben genannten Projekt wurde mir folgender Sachverhalt zur Kenntnis gegeben:

Ein Verein mit Bundeskoordinationsstelle in Berlin erteilt im Rahmen eines bundesweit durchgeführten Projekts denjenigen Schulen, die sich nach den Maßgaben des Vereins dafür qualifiziert haben, die Auszeichnung „Schule ohne Rassismus – Schule mit Courage“. Nach Angaben des Vereins wurde das Projekt 1988 in Belgien entwickelt und zwischenzeitlich in Belgien, den Niederlanden, Österreich, Spanien und Deutschland erfolgreich umgesetzt. Ziel dieses Projekts ist unter anderem die Förderung einer offenen Auseinandersetzung mit Diskriminierungen jedweder Art sowie die weitere Entwicklung von eigenen Ideen und Projekten der Schülerinnen und Schüler zur Auseinandersetzung mit Diskriminierung und Rassismus sowie Prävention und Überwindung von Rassismus.

Voraussetzung zur Erlangung der Auszeichnung „Schule ohne Rassismus – Schule mit Courage“ ist unter anderem, dass sich mindestens 70 % der Schulmitglieder (bestehend aus Schüler/-innen, Lehrer/-innen und weitere Mitarbeiter/-innen an dieser Schule) mit den Zielen des Projekts identifizieren und sich dafür einsetzen. Als Nachweis, dass diese Voraussetzung erfüllt ist, dient unter anderem eine von dem Verein den Schulen zur Verfügung gestellte „Kopiervorlage Unterschriftenliste“. Inhalt dieser Liste sind unter anderem die Vor- und Nachnamen sowie die Geburtsdaten und Unterschriften der Schulmitglieder, die das Projekt unterstützen. Die ausgefüllten und unterzeichneten Listen werden von den Schulleitungen als Anlagen zu dem jeweiligen Aufnahmeantrag zu dem Projekt „Schule ohne Rassismus – Schule mit Courage“ an die Bundeskoordinationsstelle des Vereins übermittelt. Auf meine Nachfrage teilte mir die Bundeskoordinationsstelle mit, diese Listen dienten der Überprüfung der Angaben der Schulleitungen [Erreichens des erforderlichen (Mindest-)Prozentsatzes der Unterzeichnenden] durch den Verein.

Aus datenschutzrechtlicher Sicht ist dieses Prozedere zu kritisieren:

Für diese Datenverarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO ist weder eine gesetzliche Grundlage im Hessischen Schulgesetz noch in der Daten-

schutz-Grundverordnung ersichtlich. Auch lagen die erforderlichen informierten Einwilligungen der Betroffenen hierfür nicht vor.

Art. 4 Nr. 2 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung; …

Für die Rechtmäßigkeit dieser Datenverarbeitung hätte jedoch eine Einwilligung der Betroffenen nach Art. 6 Abs. 1 lit. a DS-GVO oder eine gesetzliche Grundlage vorliegen müssen (Art. 6 Abs. 1 lit. e DS-GVO).

Art. 6 Abs. 1 lit. a und e DS-GVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

…

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; …

Weiterhin ist die vorbeschriebene Datenübermittlung durch die Schule an die Bundeskoordinationsstelle des Vereins zur Erreichung des angestrebten Zwecks nicht erforderlich und widerspricht bereits dem Grundsatz der Datenminimierung nach Art. 5 Nr. 1 lit. c DS-GVO.

Art. 5 Abs. 1 lit. c DS-GVO

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung").

Nach alledem ist dieser Datenverarbeitungsprozess der Schule sowie der Koordinationsstelle des Vereins nicht mit den datenschutzrechtlichen Bestimmungen vereinbar und somit rechtswidrig.

Zur Überprüfung der Anzahl der Unterzeichnerinnen und Unterzeichner sind die Angaben der Namen und Geburtsdaten nicht erforderlich. Vielmehr wäre eine dienstliche Erklärung der Schulleitung hinsichtlich des erreichten

Prozentsatzes der Unterstützerinnen und Unterstützer des Projekts ausreichend. Eine Überprüfbarkeit des geforderten Prozentsatzes kann mit einem anonymisierten Verfahren erfolgen. Denkbar wäre hier beispielsweise die Durchführung einer schriftlichen anonymen Umfrage innerhalb der Schule, in der die Betroffenen auf einem Fragebogen lediglich ankreuzen,

– ob sie sich mit den Zielen des Projektes identifizieren und dieses unterstützen möchten,
– ob sie das Projekt nicht unterstützen möchten oder
– ob sie sich enthalten möchten.

Diese anonymen Fragebogen könnten in der Schule aufbewahrt und der Koordinationsstelle des Vereins auf Nachfrage zur Verfügung gestellt werden. Damit wäre der Kontrollzweck erfüllt.

Meine Auffassung teilte ich sowohl der betreffenden Schule als auch dem Hessischen Kultusministerium mit und legte diesen jeweils mein soeben beschriebenes alternatives Konzept zur datenschutzkonformen Gestaltung des kritisierten Prozederes dar.

Die Schule verzichtete daraufhin auf die Verwendung der „Kopiervorlage Unterschriftenliste“. Vielmehr wurde die Zustimmung der Schülerinnen und Schüler durch Abfrage und Notierung der Anzahl der durch Handzeichen erteilten Zustimmungen durchgeführt. Auch dieses Verfahren ist jedoch nicht datenschutzkonform: Da die Abfrage in den jeweiligen Klassen nicht geheim erfolgte, steht zu befürchten, dass die Schüler/-innen sich zur Erteilung ihrer Zustimmung genötigt fühlten. Schließlich hing von ihrer Zustimmung die Erlangung der Auszeichnung „Schule ohne Rassismus – Schule mit Courage“ für die Schule ab. Die Schülerinnen und Schüler könnten daher aus Angst vor Repressalien seitens der Mitschülerinnen und Mitschüler oder negativen Konsequenzen seitens der Schule ihre Zustimmung erteilt haben. Fraglich ist mithin, ob deren Zustimmung tatsächlich in jedem Einzelfall freiwillig und damit wirksam im Sinne des Art. 4 Nr. 11 DS-GVO erteilt wurde.

Art. 4 Nr. 11 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist; …

Die betreffende Schule habe ich auch auf diesen Aspekt hingewiesen. Auch das Hessische Kultusministerium stand meiner datenschutzrechtlichen Kritik sowie meinen konzeptionellen Anregungen aufgeschlossen gegenüber. Die abschließende Abstimmung mit dem Hessischen Kultusministerium zur Änderung des kritisierten Prozederes an hessischen Schulen ist gegenwärtig noch nicht abgeschlossen.

In einem weiteren Schritt wird die bundesweite Abstimmung mit den Landesdatenschutzaufsichtsbehörden und Kultusministerien hinsichtlich einer datenschutzkonformen Gestaltung dieses Projekts anzustreben sein.

4.5
Verkehr, Daseinsvorsorge

4.5.1
Datenschutzrechtliche Zulässigkeit von Unfalldatenspeichern

Die Auslieferung eines Neuwagens an den Käufer mit einem serienmäßig eingebauten Unfalldatenspeicher bedarf keiner ausdrücklichen datenschutzrechtlichen Einwilligung des Käufers.

Mit der fortschreitenden Digitalisierung der Fahrzeuge häufen sich auch Beschwerden gegen dessen Speicher- und Assistenzsysteme. So trug eine Beschwerdeführerin vor, dass die Ausstattung eines Fahrzeugs mit einem Unfalldatenspeicher (UDS) einer ausdrücklichen Einwilligung des Käufers bedarf. Bei einer technischen Vorrichtung, die geeignet ist, persönliches Fahrverhalten des Fahrers aufzuzeichnen, sei nach datenschutzrechtlichen Vorschriften eine ausdrückliche Einwilligung zu verlangen. Sie berief sich auf das Fehlen einer solchen Einwilligung und verlangte vom Verkäufer die Rücknahme des gekauften Fahrzeugs Zug um Zug gegen die Rückzahlung des gezahlten Kaufpreises.

Ein Unfalldatenspeicher ist ein elektronisches Gerät, mit dem die vielen technischen Größen während der Fahrt je nach Einstellung für ungefähr 30 Sekunden vor und ca. 15 Sekunden nach dem auslösenden Ereignis (z. B. Unfall) dauerhaft gespeichert werden und nach einem Unfall abgerufen werden können. Auf diese Weise kann zu einem späteren Zeitpunkt das Geschehen rekonstruiert und die Schuldfrage leichter geklärt werden.

Die datenschutzrechtlichen Vorschriften enthalten kein generelles Verbot, Unfalldatenspeicher in die Fahrzeuge einzubauen. Mit welcher Ausstattung ein Fahrzeug ausgeliefert wird, ist eine Frage der kaufvertragsrechtlichen Vereinbarung. Die Kaufsache muss mit einer vereinbarten Beschaffenheit übergeben werden. Weist das ausgelieferte Fahrzeug eine andere Beschaf-

fenheit als vereinbart aus, liegt ein Mangel vor, der Sachmängelrechte nach kaufrechtlichen Vorschriften auslöst. Diese sind gegenüber dem Verkäufer des Fahrzeugs geltend zu machen und – wenn nötig – vor den Zivilgerichten auszufechten.

Die datenschutzrechtlichen Vorschriften finden erst dann Anwendung, wenn eine Person oder eine Stelle, die nicht Betroffener ist, die Daten aus dem Fahrzeug erhebt. Bei den Offline- Fahrzeugen, deren Steuergeräte also die Daten nicht aus dem Fahrzeug heraus senden, greifen die Vorschriften der Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG), wenn die Informationen – beispielsweise von der Werkstatt – aus dem Unfalldatenspeicher ausgelesen werden. Genau zu diesem Zeitpunkt müssen ihnen auch die Datenschutz-Informationen von der erhebenden Stelle zur Verfügung gestellt werden (Art. 13 Abs. 1 S. 1 DS-GVO).

Vereinzelt wird in der Presse verlangt, dass die Automobilhersteller eine Art Datenpass fürs Auto herausgeben, der über die Datenverarbeitungen im Fahrzeug aufklärt. Dies sind aber Forderungen, die an den Gesetzgeber gerichtet sind. Das geltende Datenschutzrecht kennt keine so weitgehenden Informationspflichten.

Im Rahmen eines Austauschs der unabhängigen Datenschutzaufsichtsbehörden und des Verbands der Automobilindustrie (VDA) entstand ein Mustertext zur Datenverarbeitung im Fahrzeug. Dieser enthält allgemeine Informationen und soll als Überblick über die im Auto verarbeitenden Daten dienen. Dieser Mustertext (https://datenschutz.hessen.de/datenschutz/verkehr-versorger/datenverarbeitung-im-fahrzeug) wird von den Automobilherstellern an Kontaktstellen zu den Betroffenen (z. B. in Verkaufsprospekten) platziert.

4.5.2
Gespeicherte Daten von Messgeräten – Auskunftsrecht gegenüber dem Vermieter/der Hausverwaltung

Mieter müssen ihr Auskunftsrecht über die in einem Messgerät gespeicherten Daten, die durch einen Messdienstleister im Auftrag der Vermieterin/des Vermieters bzw. der Hausverwaltung erhoben werden, gegenüber den Vermietern/den Hausverwaltungen geltend machen.

Das im Berichtszeitraum vermehrt gegenüber Auftragsverarbeitern geltend gemachte Auskunftsrecht nach Art. 15 DS-GVO gab Anlass, mich intensiv mit dieser Vorschrift zu beschäftigen.

Ein Messdienstleister war als Auftragsverarbeiter für Vermieter/Hausverwaltungen tätig und übernahm in diesem Zusammenhang Aufgaben wie

die Überprüfung, Montage und Datenverwaltung funkbasierter Messgeräte wie Heizkostenverteiler und Funkrauchmelder. Ebenso stellte er für seine Auftraggeber auch die Betriebskostenabrechnung zusammen und rechnete diese mit den jeweiligen Mietern direkt ab. Mit Geltung der Datenschutz-Grundverordnung erreichten den Messdienstleister mehrere Auskunftsanfragen gemäß Art. 15 DS-GVO von Wohnungsmietern, bei denen die Messgeräte des Messdienstleisters eingesetzt wurden. Die Mieter begehrten im Rahmen ihres Auskunftsanspruchs insbesondere Informationen zu den von den Messgeräten erfassten Daten.

Vorab ist festzustellen, dass es sich bei den von den Messgeräten erhobenen Daten um personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO handelt. Denn unter personenbezogenen Daten sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei wird eine natürliche Person bereits dann als identifizierbar angesehen, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen oder zu einer Kennnummer identifiziert werden kann.

Die Messgeräte, wie ein Heizkostenverteiler oder Funkrauchmelder, besitzen eine Gerätenummer und werden jeweils einer Wohneinheit, ggf. sogar einem Raum in der Wohneinheit zugeordnet. Die Wohneinheit ist durch Hinzuziehen weiterer Daten einem Mieter und damit einer bestimmbaren natürlichen Person zuordenbar. Darüber hinaus können beispielsweise Daten des Heizungs- und Wasserverbrauchs Aufschluss über die Anzahl der Anwesenden, die Zeiträume ihrer An- und Abwesenheit, die Nutzung bestimmter Räume sowie Rückschlüsse auf das Heizverhalten der Bewohner ermöglichen. Die Verbrauchsdaten sind daher als personenbezogene Daten anzusehen.

Gemäß Art. 15 DS-GVO hat die/der Betroffene ein Recht, vom Verantwortlichen Auskunft darüber zu erhalten, ob Daten zu ihrer/seiner Person verarbeitet werden. Ist dies der Fall, hat der Verantwortliche ihm Auskunft über diese personenbezogenen Daten sowie über die ergänzenden Informationen nach Absatz 1 zu erteilen.

Betroffenenrechte wie das Auskunftsrecht gemäß Art. 15 DS-GVO sind dabei jedoch nach dem Gesetzeswortlaut stets gegenüber dem Verantwortlichen geltend zu machen.

Verantwortlicher im Sinne der Datenschutz-Grundverordnung ist derjenige, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 4 Nr. 7 1. Halbsatz DS-GVO). Dies stellt in der vorliegenden Konstellation der Vermieter/die Vermieterin bzw. die Hausverwaltung dar. Diese bestimmen nämlich u. a., welches Gerät eingesetzt wird, in welchem Rhythmus die Er-

hebung der Zählerstände und die Erstellung der Betriebskostenabrechnung erfolgt. Der Messdienstleister, der lediglich im Auftrag für die Vermieterin/den Vermieter bzw. die Hausverwaltung Daten erhebt und verwaltet, ist in diesem Zusammenhang nur Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO. Dieser ist dem Verantwortlichen gegenüber weisungsabhängig und agiert als „unterstützendes Werkzeug“ für den Auftraggeber.

Verantwortlich für die Datenverarbeitung bleibt daher der Vermieter/die Vermieterin bzw. die Hausverwaltung. Der Auftragsverarbeiter hat lediglich die Pflicht gemäß Art. 28 Abs. 3 S. 2 lit. e DS-GVO, den Verantwortlichen in der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte zu unterstützen. Der Verantwortliche kann daher den Auftragnehmer anweisen, die notwendigen Daten und Informationen ihm gegenüber bereitzustellen, damit er seinen Mietern die Auskunft vollständig erteilen kann oder auch den Auftragnehmer mit der Erteilung der Auskunft beauftragen. Adressat des Auskunftsverlangens ist der Verantwortliche, also der Vermieter/die Vermieterin bzw. die Hausverwaltung.

Die Mieter wurden daher von mir darauf hingewiesen, dass sie ihren Auskunftsanspruch gegenüber ihren jeweiligen Vermietern/Hausverwaltungen und nicht gegenüber dem Messdienstleister als Auftragsverarbeiter geltend machen müssen.

4.5.3
Ergebnisse der Prüfung zur Einhaltung datenschutzrechtlicher Vorschriften durch die Autowerkstatt

Moderne Kraftfahrzeuge generieren immer mehr Daten. Viele davon werden in der Werkstatt für die Inspektion, den Service oder die Reparatur benötigt. Auch rein technische Daten sind personenbezogene Daten, wenn sie über die Fahrzeugidentifikationsnummer mit den Halterdaten oder den Kundendaten verknüpft werden. Im Juni 2017 startete dazu eine bundesweite Prüfung von Autowerkstätten durch sechs Aufsichtsbehörden, um die Verarbeitung von Fahrzeugdaten nachzuvollziehen und auf die datenschutzrechtliche Relevanz und Vereinbarkeit zu untersuchen, auf die sich dieser gemeinsame Bericht bezieht.

Von meiner Dienststelle wurden 20 Werkstätten zur Beantwortung eines umfangreichen Fragenkatalogs aufgefordert. Zehn der geprüften Werkstätten waren die eines in Hessen ansässigen Automobilherstellers, weitere zehn Vertragswerkstätten von verschiedenen Automobilimporteuren.

Dabei wurden die Werkstätten unter anderem befragt, welche personenbezogenen Daten aus dem Fahrzeug bei einem Werkstattbesuch ausgelesen und in dem Datenverarbeitungssystem der Werkstatt gespeichert werden. Zentrale Themen der Befragung waren die Rechtsgrundlage für die Datenverarbeitung, die Weitergabe der Daten an den Hersteller oder an andere Dritte wie beispielsweise Versicherungen und die Information der Kunden über eine Verarbeitung ihrer Kraftfahrzeugdaten. Die Antworten der Werkstätten aller teilnehmenden Bundesländer wurden anonymisiert ausgewertet.

Das Ergebnis zeigte, dass die Datenverarbeitung der zwingend für Reparatur, Service und Wartung erforderlichen Daten inklusive Datenübermittlung an den Hersteller gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO zulässig ist. Für eine Einwilligung in die Datenverarbeitung besteht in diesen Fällen keine Notwendigkeit. Einige Werkstätten hatten trotzdem eine Einwilligung für eine Datenverarbeitung vorgelegt, die jedoch so weit gefasst war, dass pauschal in jedwede Datenverarbeitung eingewilligt werden sollte. Diese Einwilligung war auch verknüpft mit der Auftragsannahme. Diese Vorgehensweise verstößt jedoch gegen die datenschutzrechtlichen Regelungen. Zum einen muss die Einwilligung in die Datenverarbeitung zweckgebunden sein. Es muss aus der Erklärung ersichtlich sein, welche Daten zu welchem Zweck erhoben werden und wie sie verarbeitet werden. Zum anderen muss die Abgabe einer Einwilligung freiwillig sein, sie darf also an keine nachteiligen Folgen gekoppelt werden. Die Annahme des Kraftfahrzeugs zur Reparatur darf nicht davon abhängig gemacht werden, ob der Kunde die Einwilligung unterschreibt.

Die DS-GVO schreibt vor, dass der Kunde in präziser, transparenter, verständlicher und leicht zugänglicher Art und Weise Informationen erhält, die sich auf die Verarbeitung beziehen. Die Werkstätten gaben an, dass Informationen zur Datenverarbeitung entweder in den Betriebsanleitungen oder in den Einwilligungserklärungen vorhanden seien oder die Kunden durch Servicemitarbeiter aufgeklärt würden. Ich empfahl den Werkstätten, ein Informationsblatt zur Datenverarbeitung an die Kunden mit dem Inhalt gemäß Art. 12, 13 DS-GVO auszuhändigen oder auf dem Auftrag mit aufzudrucken.

Schwieriger zu beantworten war die Frage, auf welchen rechtlichen Grundlagen die Verknüpfung der technischen Daten mit dem Namen des Kunden oder mit der Fahrzeugidentifikationsnummer übermittelt werden darf. Viele der Übermittlungen erfolgen aufgrund der Vertragserfüllung im Rahmen des Werkstattvertrages gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO. Darunter fällt beispielsweise bei Garantie-, Gewährleistungs- und Kulanzfällen die Prüfung der Leistungserstattung durch die Hersteller und die Konsultation der Hersteller bei besonderen Schwierigkeiten im Rahmen der konkreten Reparaturdurchführungen (technische Hotline, Fahrzeugdiagnose/Telediagnose).

Die datenschutzrechtliche Grundlage für die Datenverarbeitung der erforderlichen Fahrzeugdaten für die Produktüberwachung/Produktbeobachtung und für eventuelle Rückrufaktionen ist Art. 6 Abs. 1 Satz 1 lit. c DS-GVO. Es liegt hier die Erfüllung einer rechtlichen Verpflichtung des Automobilherstellers aus dem Produkthaftungsgesetz vor. Da hier Konstellationen denkbar sind, in denen sowohl die Werkstatt als auch der Hersteller dieselben Daten der Kunden für jeweils eigene Zwecke verarbeiten, wäre eine gemeinsame Verarbeitung gemäß Art. 26 DS-GVO denkbar, mit der Konsequenz, dass die Werkstätten und die Hersteller in einer gemeinsamen Vereinbarung festlegen, wer welchen Informationspflichten nachkommt.

Für eine Datenverarbeitung zu Zwecken der Produkt-/Qualitätsverbesserungen und Produktfortentwicklungen kann Art. 6 Abs. 1 Satz 1 lit. f DS-GVO herangezogen werden. Gleiches gilt für Datenverarbeitungen im Kontext von Marketing-Aktionen und Kundenzufriedenheitsbefragungen. Diese könnten jedoch auch anonymisiert verarbeitet werden.

Demgegenüber kann die zentrale Führung einer elektronischen Wartungs- und Reparaturhistorie beim Automobilhersteller (digitaler Servicenachweis) nur mit expliziter Einwilligung des Halters durchgeführt werden. Gleiches gilt für die Teilnahme an Vergütungs- und Bonusprogrammen der Kunden.

Die Prüfung hat gezeigt, dass die Werkstätten sich kaum bewusst sind, welche Daten sie für welche Zwecke erheben und an die Hersteller weiterleiten. Die Datenverarbeitung für eigene Zwecke und für Zwecke, die dem Hersteller dienen, werden als nicht getrennt voneinander wahrgenommen. Somit fehlt es auch oftmals an einer ordnungsgemäßen Information der Kunden und an einer ordnungsgemäßen Vereinbarung zwischen Werkstätten und Herstellern.

4.6
Gesundheitswesen

4.6.1
Prüfung der Informationen nach Art. 13 DS-GVO im Gesundheitsbereich

Informationen nach Art. 13 DS-GVO müssen vor allem bestimmt und transparent sein. Im Gesundheitsbereich ist die Information den Betroffenen grundsätzlich in Papierform mitzuteilen, sodass diese die Möglichkeit haben, sie zur weiteren Ansicht mitzunehmen. Zudem sind Einwilligungen von den Informationen nach Art. 13 DS-GVO zu trennen.

Im Rahmen von Beschwerden und Beratungsfragen wurden mir zahlreiche Dokumente zur Erfüllung der Pflicht nach Art. 13 DS-GVO zur Prüfung vorge-

legt. Dabei handelte es sich um Unterlagen aus den unterschiedlichsten Gesundheitsbereichen, wie z. B. von (Zahn-)Arztpraxen, Psychotherapeut/-innen, Krankenhäusern, Sanitätshäusern, Physiotherapeut/-innen, Pflegediensten, Heilpraktiker/-innen, ärztlichen Verrechnungsstellen und Gesundheitsämtern.

Bei der Prüfung stellte sich heraus, dass bei der Erstellung der Informationsflyer zum großen Teil die gleichen Fehler gemacht werden.

So musste ich oft darauf hinweisen, dass die Informationen den Patientinnen und Patienten bzw. Kundinnen und Kunden in Papierform zur Verfügung zu stellen sind. Da es sich im Gesundheitsbereich grundsätzlich um persönlich zu schließende (Behandlungs-)Verträge handelt, reicht eine Information auf der Homepage des Verantwortlichen allein nicht aus. Aber auch ein Aushang genügt – entgegen weitverbreiteter Ansicht – nicht dem Erfordernis der „leicht zugänglichen Form“ des Art. 12 Abs. 1 DS-GVO. Aus meiner Sicht ist jedoch ein Medienbruch in der Form zulässig, dass im Flyer auf umfangreichere Informationen im Internet verwiesen wird.

Für grundsätzlich unzulässig halte ich den Ansatz, Informationen nach Art. 13 DS-GVO mit Einwilligungserklärungen zu vermengen. Hier wird in der Regel in einem Dokument nach Art. 13 informiert und am Ende die Einwilligung in die, im gesamten Dokument aufgezählte, Datenverarbeitung gefordert. Von den Verantwortlichen werden hierfür die Argumente der „Einfachheit“ und der „Papiersparsamkeit“ ins Feld geführt. Zudem wird argumentiert, dass man die Patientinnen und Patienten bzw. Kundinnen und Kunden nicht mit zu viel Bürokratie „überfrachten“ möchte. Dabei wird jedoch übersehen, dass die Daten im Behandlungskontext grundsätzlich auf der Grundlage von Art. 9 Abs. 2 lit. h DS-GVO verarbeitet werden. Eine Einwilligung in die Verarbeitung ist somit nicht erforderlich. Die Informationen nach Art. 13 DS-GVO über die Verarbeitung müssen hingegen betreffend aller Arten von Verarbeitungen mitgeteilt werden, unabhängig davon, ob diese aufgrund einer gesetzlichen Grundlage oder einer Einwilligung erfolgen. Bei der Vermengung wird der Betroffene somit meist dazu veranlasst, in eine gesetzlich erlaubte Verarbeitung einzuwilligen. Im Übrigen führt eine solche Vermengung dazu, dass die in Art. 12 Abs. 1 DS-GVO genannten Grundsätze der transparenten, verständlichen und leicht zugänglichen Form der Informationen oft nicht eingehalten werden können. Den Betroffenen wird es in den Fällen gerade schwer gemacht zu differenzieren, welche Verarbeitungsvorgänge sie durch seine Einwilligung beeinflussen können.

Getroffene Maßnahmen

Ich habe die Prüfungen zum Anlass genommen, diese und weitere Fehler in einer „Checkliste zur Verhinderung der häufigsten Fehler bei der Anwendung des Art. 13 DS-GVO im Gesundheitsbereich“ zusammenzufassen. Diese Liste habe ich auf meiner Homepage unter dem Link: https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/checkliste-zur-verhinderung-der-häufigsten als Praxishilfe veröffentlicht.

4.6.2
Nichtbehandlung im Fall der Weigerung von Patientinnen und Patienten, den Info-Flyer nach Art. 13 DS-GVO zu unterzeichnen

Ärztinnen und Ärzte sowie andere Angehörige von Gesundheitsberufen dürfen nicht die Behandlung ablehnen, abbrechen oder dies androhen, wenn die Patientin oder der Patient sich weigert, die Information nach Art. 13 DS-GVO zu unterzeichnen.

Nach der Einführung der Pflicht durch die DS-GVO, die betroffene Person über die Verarbeitung ihrer personenbezogenen Daten nach Art. 13 DS-GVO zu informieren, wurden mir zahlreiche Fälle gemeldet, in denen Ärztinnen und Ärzte den Patientinnen und Patienten die (weitere) Behandlung verweigerten, weil diese den Erhalt bzw. die Kenntnisnahme der Information nach Art. 13 DS-GVO nicht mit Unterschrift bestätigen wollten.

In diesen Fällen wurde das Papier meist nach Erteilung der Unterschrift wieder zur Dokumentation des Arztes genommen, ohne dass der Patient eine Kopie der Information erhielt. Auch wurde mir in vielen Fällen zugetragen, dass das Praxispersonal entnervt auf Fragen zum Papier und nach dem Zweck der Unterschrift reagiere. Auch auf Nachfrage wurde das Papier den Patientinnen und Patienten nicht erläutert. In diesen Fällen wurde den Patientinnen und Patienten dann mitgeteilt, eine Behandlung wäre ohne die Unterschrift der Information nicht möglich.

Schon vor der Geltung der DS-GVO bestand unter den Aufsichtsbehörden Einigkeit darüber, dass eine Unterschrift für den Nachweis der Erteilung der Information nach Art. 13 DS-GVO nicht erforderlich ist. Dem Patienten muss die Information nach Art. 13 DS-GVO mitgeteilt werden, eine Annahmepflicht besteht für den Betroffenen aber nicht. Darauf habe ich auch in meinem Informationspapier zur „Umsetzung der Informationspflichten nach Art. 12 und 13 DS-GVO im Bereich der Gesundheitsberufe“ auf meiner Homepage hingewiesen (https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/info-pflichten-nach-ds-gvo). Aus meiner

Sicht genügt es für den Nachweis der Erteilung der Information, dass die Erteilung vom Verantwortlichen vermerkt oder ein konkreter Verfahrensablauf betreffend die Umsetzung der Informationspflicht schriftlich festgehalten wird.

Ärztinnen und Ärzte dürfen daher die Behandlung bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Information nach Art. 13 DS-GVO durch Unterschrift zu bestätigen, nicht ablehnen.

Nicht ganz unproblematisch ist es jedoch, dass die Frage der Behandlungsverweigerung an sich nicht datenschutzrechtlicher Natur ist, sondern die Ausgestaltung der Vertragsfreiheit zwischen den Angehörigen der Gesundheitsberufe und den Patientinnen und Patienten betrifft. Nach Art. 7 Abs. 2 Satz 2 der Berufsordnung für die Ärztinnen und Ärzte in Hessen kann die Ärztin oder der Arzt die Behandlung einer Patientin oder eines Patienten ablehnen, sofern nicht ein Notfall oder eine besondere rechtliche Verpflichtung zur Behandlung vorliegt. Ich habe daher die Problematik mit der Landesärztekammer Hessen besprochen, mit dem Ergebnis, künftig Fälle der Behandlungsverweigerung an sie weiterzugeben.

In den mir gemeldeten Fällen der Behandlungsverweigerung habe ich mir von den Verantwortlichen die Informationspapiere nach Art. 13 DS-GVO vorlegen lassen und sie auf meine Rechtsansicht hingewiesen. In allen Fällen waren die Ärztinnen und Ärzte einsichtig und haben ihre Informationspapiere überarbeitet. Die Behandlungsverweigerung oder die Drohung damit wurde hingegen meist bestritten.

Aufgrund der Häufung derartiger Fälle habe ich ergänzend auf einen Beschluss der DSK hingewirkt (https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_aerzte.pdf).

4.7
Wirtschaft, Vereine

4.7.1
Die Umsetzung der DS-GVO in kleinen und mittleren Unternehmen

Die Reform des Datenschutzrechts hat besonders bei kleinen und mittleren Unternehmen zu großer Unsicherheit und nicht selten auch zu Überforderung geführt. Dies zeigte sich im Berichtszeitraum einerseits an der stark gestiegenen Zahl an Beschwerden, vor allem aber an hunderten von telefonischen und schriftlichen Beratungsanfragen kleiner Unternehmen aus allen Branchen (Handel, Handwerk, Industrie, Dienstleister etc.). Die meisten Fragen und Sorgen der kleinen Unternehmen drehten sich dabei stets um die gleichen Themen.

Über 99 % der Unternehmen in Deutschland zählen zu den sogenannten kleinen und mittleren Unternehmen (KMU), die höchstens 250, häufig jedoch noch deutlich weniger Mitarbeiter haben. Obwohl das Datenschutzrecht schon seit Jahrzehnten auch für kleine und mittlere Unternehmen gilt, zeigte sich bei meiner Aufsichtspraxis leider immer wieder, dass von diesen dem Datenschutz häufig keine allzu große Bedeutung beigemessen wurde. Lediglich bei solchen kleinen Unternehmen, deren Geschäftszweck gerade die Verarbeitung von Daten ist, nahm und nimmt die Beachtung der datenschutzrechtlichen Anforderungen regelmäßig einen hohen Stellenwert ein. Der weit überwiegende Teil der kleinen und mittleren Unternehmen verarbeitet personenbezogene Daten jedoch nur als Mittel zum Zweck, um die eigentliche Tätigkeit des Unternehmens effektiv ausüben zu können bzw. um die Verwaltung der Kunden-, Mitarbeiter- und sonstigen geschäftlichen Daten zu organisieren. Bei diesen Unternehmen fehlte in der Vergangenheit häufig das Bewusstsein und teilweise auch das Verständnis dafür, dass das Datenschutzrecht mit seinen vielfältigen Anforderungen auch für ihre Tätigkeiten gilt.

Mit der Reform des Datenschutzrechts und der Geltung der DS-GVO seit Mai 2018 rückte das Thema jedoch auch bei kleinen und mittleren Unternehmen plötzlich stark in den Fokus. Dies war sicherlich auch der umfangreichen medialen Berichterstattung geschuldet, die (nicht selten in überdramatisierender Form) Probleme und mögliche Folgen des neuen Datenschutzrechts beschwor. Obwohl der europäische Gesetzgeber vom Inkrafttreten der DS-GVO bis zu deren Geltung eine Frist von zwei Jahren zur Vorbereitung auf die neuen Regeln vorgesehen hatte, erkannten gerade viele kleine Unternehmen erst wenige Wochen vor deren Geltung bzw. teilweise sogar erst danach die Dringlichkeit der Umsetzung. So sind viele Unternehmen, die das Thema Datenschutz bisher ganz ignoriert oder weitgehend vernachlässigt haben, im Laufe des Jahres 2018 aufgewacht und haben sich erstmals, oder zumindest erstmals im erforderlichen Umfang, mit ihren datenschutzrechtlichen Verpflichtungen befasst. Dies kann sicherlich als einer der Erfolge der Datenschutzreform gewertet werden.

In unzähligen schriftlichen und mehreren hundert telefonischen Anfragen haben kleine und mittlere Unternehmen Fragen zum Datenschutz gestellt und meine Behörde um Beratung zur Umsetzung des neuen Datenschutzrechts in ihren Betrieben ersucht. Zudem haben meine Mitarbeiter bei diversen Vorträgen und Workshops, die sich primär an kleine und mittlere Unternehmen richteten, umfangreich Tipps und Hinweise zur Umsetzung der neuen Regeln gegeben. Die Fragen, die dabei von den Unternehmen gestellt wurden, waren zumeist sehr grundlegender Art und wiederholten sich inhaltlich immer wieder:

– Benötigt das Unternehmen einen betrieblichen Datenschutzbeauftragten?
– Welche Informationspflichten gibt es und wie müssen diese erfüllt werden?
– Für welche Vorgänge wird eine ausdrückliche Einwilligung der Betroffenen benötigt und wie muss diese aussehen?
– Welche technischen Anforderungen gibt es für bestimmte Verarbeitungen?
– Was ist eine Auftragsverarbeitung und in welchen Fällen liegt sie vor?
– Was ist das Verzeichnis von Verarbeitungstätigkeiten?
– Welche Folgen und Sanktionen drohen einem Unternehmen bei Verstößen?

In der Beratungspraxis wurde offenbar, dass viele kleine und mittlere Unternehmen bisher wenig bis gar keine Erfahrungen mit dem Thema Datenschutz gemacht hatten. Obwohl sich viele Anforderungen gegenüber der alten Rechtslage kaum geändert haben, wurde sehr häufig nach datenschutzrechtlichen Grundsätzen gefragt, die schon seit Jahren nahezu unverändert gelten und die dementsprechend eigentlich schon seit langem von den Unternehmen hätten beachtet werden müssen. Viele Fragen wurden auch zu Formalitäten gestellt, die mit der DS-GVO neu eingeführt oder geändert wurden. Letzteres legte teilweise die Vermutung nahe, dass manche Unternehmen zwar bestimmte, verhältnismäßig einfach umzusetzende formelle Anforderungen erfüllen wollten, die Grundlagen des Datenschutzrechts aber leider wenig beachteten oder verstanden hatten.

Häufig wurden von den kleinen und mittleren Unternehmen auch Sorgen und Ängste einerseits vor zusätzlichem bürokratischem Aufwand und andererseits vor vermeintlichen Millionenbußgeldern und teuren Abmahnungen geäußert. Besonders die Furcht vor letzterem, geschürt durch reißerische Berichterstattung und unseriöse Berater, resultierte oft in Rat- und Hilflosigkeit, teilweise auch in übertriebenem Aktionismus bzw. Resignation. In einigen Fällen schlug meinen Mitarbeitern auch deutlicher Unmut über die neuen Regeln und den damit einhergehenden Aufwand bei der Umsetzung entgegen, dies vereinzelt auch in sehr derber und unhöflicher Form.

Die große Rechtsunsicherheit, die bei vielen kleineren Unternehmen herrschte und teilweise noch immer herrscht, ging nicht selten mit der Erwartung einher, von der Aufsichtsbehörde umfassend beraten und unterstützt zu werden. Angesichts der Flut der Anfragen war und ist es mir und meinen Mitarbeitern allerdings nicht möglich, alle anfragenden Unternehmen in dem von ihnen gewünschten Umfang individuell zu ihren Datenschutzfragen zu beraten. Auf der Webseite meiner Behörde biete ich zu verschiedenen datenschutzrechtlichen Themen und insbesondere zur Datenschutzreform eine Vielzahl allgemeiner Hinweise, grundlegender Papiere, hilfreicher Tipps sowie Antworten auf häufig gestellte Fragen an, die sich u. a. auch an kleine und mittlere Unternehmen

richten. Daneben finden die Unternehmen vor allem bei ihren jeweiligen betrieblichen Datenschutzbeauftragten sowie bei externen Datenschutzberatern Unterstützung und individuelle Beratung. Auch viele Verbände und Kammern unterstützen ihre Mitgliedsunternehmen mit branchenspezifischen Informationen bei der Umsetzung der datenschutzrechtlichen Anforderungen.

Gegen Ende des Jahres 2018 ließ die Zahl an Beratungsanfragen von kleinen und mittleren Unternehmen etwas nach, wobei sie aber das Niveau der Vorjahre noch immer deutlich überstieg. Ob der Rückgang darauf zurückzuführen ist, dass die Unternehmen nunmehr beim Datenschutz besser aufgestellt sind, oder darauf, dass die zwischenzeitliche Panik bei diesem Thema wieder abgeflacht ist, ist nicht feststellbar. In den meisten kleinen und mittleren Unternehmen dürfte der Datenschutz im Laufe des Berichtszeitraums jedenfalls verstärkt ins Bewusstsein gerückt sein und viele Unternehmen haben bereits gute Arbeit bei der Umsetzung des neuen Datenschutzrechts geleistet.

4.7.2
Rechte betroffener Personen nach der DS-GVO gegenüber Rechtsanwälten

Betroffene Personen können gegenüber Rechtsanwälten ihre Rechte nach der DS-GVO geltend machen. Allerdings können mit Informations- oder Auskunftsansprüchen nicht die Gegenseite und die gegnerischen Rechtsanwälte ausgeforscht werden.

Mich erreichten mehrere Beschwerden, in denen die Betroffenen Informationen und Auskünfte nach der DS-GVO über ihre personenbezogenen Daten bei Rechtsanwälten begehrten.

So schrieb mir unter anderem ein Petent, dass der Rechtsanwalt ihm keine Datenschutzerklärung geschickt und ihn somit nicht über seine Rechte und Pflichten aus der DS-GVO informiert habe. Ein anderer Petent monierte, dass seine an die Rechtsanwaltskanzlei gerichteten Anfragen trotz Berufung auf das neue Datenschutzrecht ohne Erfolg geblieben seien. Häufig fehlten in den Beschwerden jedoch Ausführungen dazu, in welchem Verhältnis die Petenten zu den Rechtsanwälten stehen – ob es sich etwa um die eigenen Rechtsanwälte oder um Rechtsanwälte der Gegenseite handelt.

Sofern mit den Rechtsanwälten ein Mandatsverhältnis besteht, können Mandanten ihre Rechte aus der DS-GVO gegenüber diesen geltend machen. Hierbei ist jedoch zu beachten, dass Rechtsanwälte grundsätzlich die personenbezogenen Daten im Rahmen eines Mandatsverhältnisses verarbeiten

dürfen, da die Verarbeitung zur Wahrung der berechtigten Interessen der Mandanten erforderlich ist (vgl. Art. 6 Abs. 1 lit. f DS-GVO).

Sofern kein Mandatsverhältnis mit der betroffenen Person besteht, können die Rechtsanwälte aufgrund der anwaltlichen Verschwiegenheitspflicht gemäß § 43a Abs. 2 Bundesrechtsanwaltsordnung (BRAO) die Informationen gemäß Art. 14 Abs. 5 lit. d DS-GVO unterlassen sowie die Auskunft gemäß § 29 Abs. 1 Satz 2 BDSG verweigern. Art. 14 Abs. 5 lit. d DS-GVO sieht vor, dass die Pflicht zur Information gemäß Art. 14 Abs. 1 bis 4 DS-GVO nicht besteht, wenn und soweit die personenbezogenen Daten gemäß dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Art. 14 Abs. 5 lit. d DS-GVO

Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

…

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Des Weiteren sieht § 29 Abs. 1 Satz 2 BDSG vor, dass das Recht auf Auskunft gemäß Art. 15 DS-GVO dann nicht besteht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach geheim gehalten werden müssen. Ein solches Recht bzw. eine solche Rechtsvorschrift stellt die BRAO und die in ihr geregelte Verschwiegenheitspflicht des Rechtsanwalts gemäß § 43a BRAO dar.

§ 29 Abs. 2 BDSG regelt darüber hinaus die Einschränkung der Informationspflicht gemäß Art. 13 Abs. 3 DS-GVO und betrifft die Rechtsbeziehung zwischen den Mandanten der Rechtsanwälte und betroffenen dritten Personen, deren personenbezogene Daten im Rahmen des Mandatsverhältnisses an die Rechtsanwälte weitergegeben werden. Die Einschränkung der Informationspflicht der Mandanten gegenüber den betroffenen dritten Personen dient dem Schutz der ungehinderten Kommunikation zwischen Mandanten und Rechtsanwälten.

§ 29 BDSG

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten

Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

Daher konnte ich den Petenten in vielen Fällen nur mitteilen, dass keine datenschutzrechtlichen Verletzungen vorliegen und die Rechtsanwälte die Informationen unterlassen sowie die Auskünfte verweigern durften.

4.7.3
Direktwerbung nach der Datenschutz-Grundverordnung

Die Datenschutzbehörden haben die „Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke“ überarbeitet. Ergebnis ist die Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO).

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat am 07.11.2018 die Orientierungshilfe beschlossen.

Sie wendet sich gleichermaßen an Betroffene wie an Werbetreibende und den Adresshandel und ist als „Nachfolgerin“ der „Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke“ zu verstehen, die im September 2014 unter Geltung des Bundesdatenschutzgesetzes a. F. (BDSG a. F.) veröffentlicht worden war.

Bei einer vergleichenden Betrachtung der neuen mit der alten Rechtslage fällt auf, dass die DS-GVO eine vorrangige Spezialregelung, wie sie in § 28

Abs. 3 BDSG a. F. vorgesehen war, nicht kennt. Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten ist nun eine Interessenabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO, in die auch die vernünftigen Erwartungen einer betroffenen Person einzubeziehen sind.

Werden die allgemeinen Grundsätze nach Art. 5 DS-GVO „faire Verfahrensweise", „dem Verarbeitungszweck angemessen" und „in nachvollziehbarer Weise" beachtet und die Informationspflichten nach Art. 13 und 14 DS-GVO erfüllt, werden die vernünftigen Erwartungen in der Regel ausreichend berücksichtigt sein.

Art. 6 Abs. 1 lit. f DS-GVO stellt den zentralen Erlaubnistatbestand für die Datenverarbeitung im werbewirtschaftlichen Bereich dar. Die Regelung ist für jede Verarbeitung im Sinne von Art. 4 Nr. 2 einschlägig. Sie erfasst die Datenverarbeitung für eigene Werbezwecke wie für Werbezwecke Dritter und gleichermaßen auch die geschäftsmäßige Datenverarbeitung zum Zweck der Übermittlung und den Adresshandel.

Der europäische Gesetzgeber hat mit Erwägungsgrund (ErwG) 47, Satz 7, bereits eine Interessenabwägung zu Gunsten der Werbewirtschaft getroffen, davon ausgehend, dass eine tendenziell geringe Schutzbedürftigkeit für öffentlich zugängliche Adressdaten besteht, jedenfalls diese nicht die grundrechtlich gesicherten Positionen des Werbetreibenden aus Art. 12 und 14 GG sowie Art. 15, 16 und 17 GRCh (Berufsfreiheit, unternehmerische Freiheit, Eigentumsfreiheit) überwiegt. Ein Korrektiv hierzu hat der Gesetzgeber mit Art. 21 Abs. 2 DS-GVO geschaffen, wo den Betroffenen ein jederzeitiges Widerspruchsrecht eingeräumt wird.

Eine Interessenabwägung wird nach Ansicht der Aufsichtsbehörden dann nicht zu Gunsten der/des Werbetreibenden ausfallen, wenn Daten aus einem Online-Impressum zum Zweck der werblichen Nutzung ausgelesen werden. Zwar sind diese Daten allgemein zugänglich, werden aber nicht freiwillig, sondern aufgrund gesetzlicher Verpflichtung veröffentlicht.

Künftig wird eine Kompatibilitätsprüfung bei Zweckänderung gemäß Art. 6 Abs. 4 DS-GVO erforderlich.

Hinzugekommen ist auch die Pflicht des Verantwortlichen, Betroffenen die Ausübung ihrer Rechte zu erleichtern (Art. 12 Abs. 2 Satz 1 DS-GVO). Hieraus wird abgeleitet, dass für das Einlegen eines Werbewiderspruchs (auch) ein elektronischer Kommunikationsweg anzubieten ist. Ferner, dass Dateneigner und Werbender zusammenwirken. Die Information über den Werbewiderspruch ist daher vom Dateneigner ggf. an den/die Werbenden weiterzugeben.

Auch Negativauskünfte, d. h. die Auskunft, dass keine Daten gespeichert sind, sind künftig gemäß Art. 15 DS-GVO zu erteilen.

Der vollständige Text der Orientierungshilfe „Werbung“ ist abrufbar unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/OH_Werbung_Stand_07.11.2018_1.pdf

4.7.4
Entwicklung der Beachtung von Datenschutz bei Vereinen

Die europäische Datenschutz-Grundverordnung hat bei Vereinsvertretern, Verbandsfunktionären und auch Vereinsmitgliedern zu Aufregung und Unsicherheit geführt. Dabei hat die DS-GVO, entgegen der allgemeinen Auffassung, bei den Vereinen nur in wenigen Bereichen zu wirklich substanziellen Veränderungen der datenschutzrechtlichen Anforderungen geführt.

Die elektronische Datenverarbeitung bietet im Rahmen der Vereins- und Verbandsarbeit ungeahnte Möglichkeiten bei der optimalen Mitgliederbetreuung im Rahmen der Vereinsführung sowie der Organisation des Vereinslebens, wie z. B. Veranstaltungen und einen Ligabetrieb. Aufgrund des erforderlichen zeitlichen Umfangs des persönlichen Engagements ist man in vielen Vereinen und Verbänden bestrebt, die Aufgaben auf möglichst viele Beteiligte zu verteilen. Hierdurch ergeben sich bei der Vereinsarbeit vielfältige Berührungspunkte mit den Vorschriften des Datenschutzrechts.

Die DS-GVO ist seit dem 25.05.2018 in der gesamten Europäischen Union anwendbar. Sie gilt für jede Art der Verarbeitung personenbezogener Daten durch Organisationen. Lediglich im privaten und familiären Bereich ist die DS-GVO nicht anzuwenden. Damit gilt die DS-GVO auch für Vereine.

Daten sind dann personenbezogen, wenn sie sich auf eine identifizierbare Person beziehen. In Vereinen werden dies in der Regel die Daten der eigenen Mitglieder oder der Mitglieder anderer Vereine, z. B. bei Wettkämpfen, sein. Eine Verarbeitung der Daten liegt in jeder Form ihrer Nutzung vor, sei dies durch die Erhebung und Speicherung, durch das Anzeigen oder die Weitergabe an andere Mitglieder oder Trainer oder durch die Einziehung von Beiträgen. Auch das Löschen stellt eine Verarbeitung dar. Jeder Verein verarbeitet also personenbezogene Daten.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn es dafür eine ausdrückliche Rechtsgrundlage gibt. Die möglichen Rechtsgrundlagen sind in Art. 6 DS-GVO enthalten. In der Regel ist die Verarbeitung der Daten in dem Umfang zulässig, wie dies für den Vereinszweck erforderlich ist. Dies

umfasst die Buchhaltung, die Mitgliederverwaltung und die Durchführung der Vereinsaktivitäten.

Darüber hinaus können die Daten verarbeitet werden, wenn dies die Interessen des Vereins durch die Satzung erfordern und die Rechte der betroffenen Personen nicht entgegenstehen. Hierfür ist eine Interessenabwägung erforderlich.

Für die Verarbeitung personenbezogener Daten, die nicht unbedingt erforderlich ist, kann die betroffene Person eine Einwilligung erteilen. Eine Einwilligung kann nur freiwillig, d. h. ohne Zwang, erteilt werden. Einwilligungen müssen ausdrücklich erteilt werden. Vorausgefüllte Kreuze sind hierbei nicht zulässig. Die Einwilligung ist außerdem frei widerruflich. Deshalb ist es nicht möglich, Einwilligungen in Mitglieds- oder Teilnahmeanträgen oder in der Satzung ohne die Möglichkeit aufzunehmen, die Zustimmung nicht zu erteilen. Die Einwilligung ist daher für alle Verarbeitungen, die zwingend notwendig sind, keine geeignete Rechtsgrundlage.

Wichtig ist außerdem, dass die betroffenen Personen über den Umfang der Verarbeitung detailliert informiert werden. Dies kann in einem Infoblatt und den Mitgliedsanträgen erfolgen. Der genaue Umfang der notwendigen Informationen ergibt sich aus den Art. 12, 13 und 14 DS-GVO.

Um die Anforderungen der DS-GVO erfüllen zu können, muss zunächst ermittelt werden, welche personenbezogenen Daten aktuell in welchem Arbeitsablauf verarbeitet und gespeichert werden. Für jeden Verarbeitungsschritt kann dann übersichtlich geprüft werden, ob dieser für die Vereinszwecke notwendig ist und wer die Daten verarbeiten darf. Das Ergebnis kann dazu genutzt werden, die Verpflichtung zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu erfüllen und auch den entsprechenden Datenschutzhinweis nach Art. 13 und 14 DS-GVO richtig zu erstellen.

Die Benennung eines Datenschutzbeauftragten ist ab zehn Personen notwendig, die ständig mit der automatisierten Datenverarbeitung befasst sind. Dies sind vor allem die Vereinsorgane sowie Personen in der Buchhaltung, aber auch Trainer und Betreuer, denen Mitglieder- oder Spielerlisten elektronisch zur Verfügung gestellt werden. Auch wenn ein Datenschutzbeauftragter nicht zwingend erforderlich ist, kann dieser zur Beachtung der DS-GVO sehr nützlich sein.

Zudem ist zu prüfen, ob die Datensicherheit im Vereinsleben gewährleistet ist. Hierzu empfiehlt sich eine Bestandsaufnahme der Geräte, auf denen Daten gespeichert sind, und die Prüfung der Zugriffsrechte. Mobile Geräte wie Laptops sollten mit einer Verschlüsselungssoftware ausgerüstet wer-

den. Werden die Daten des Vereins auf Geräten verarbeitet, die auch von Nichtvereins- oder Vorstandsmitgliedern (z. B. Familien-PC des Ersten Vorsitzenden) genutzt werden, dürfen die Vereinsdaten den anderen Nutzern nicht zugänglich sein. Dies kann durch die Verschlüsselung der Daten oder deren Speicherung in einem geschützten Bereich erfolgen.

Trotz der im Wesentlichen unveränderten Rechtslage wurde über das Inkrafttreten der DS-GVO umfangreich berichtet. Dies hat zu einer Steigerung der Wahrnehmung des Datenschutzes bei Vereinsvertretern geführt. Leider hat dies auch zu einigen Handlungen bei der Gestattung und Verwendung von Fotografien geführt, die durch die DS-GVO nicht gerechtfertigt sind.

Vereine und deren Mitglieder möchten ihre Ergebnisse gerne in Schrift und Bild veröffentlichen. Dabei sind die Interessen der betroffenen Personen zu berücksichtigen. Haben die betroffenen Personen in die Veröffentlichung von Text und Bildern eingewilligt, ist diese zulässig. Eine Einwilligung kann in Teilnahmeanträgen oder Spielerpässen enthalten sein. Die Einwilligungen müssen allerdings freiwillig erteilt werden und dürfen daher weder zwangsweise noch verdeckt enthalten sein.

Über öffentliche Veranstaltungen darf auch ohne ausdrückliche Einwilligung textlich und bildlich berichtet werden, wenn dabei die Veranstaltung im Vordergrund steht und Einzelpersonen nicht abgebildet werden. Ohne Einwilligung dürfen auch Ergebnisse veröffentlicht werden. Die Berichterstattung darf aber nur so lange erfolgen, wie ein Interesse der Öffentlichkeit daran besteht, also für einen sehr begrenzten Zeitraum. Eine dauerhafte Veröffentlichung ohne Einwilligung scheidet damit aus.

Für Vereine sind teils noch erhebliche Anpassungsarbeiten erforderlich. Diese resultiert jedoch vor allem daraus, dass viele Vereine vor dem Inkrafttreten der DS-GVO weit entfernt davon waren, die Anforderungen der früher geltenden Regelungen aus dem BDSG a. F. zu erfüllen. Daraus ergab und ergibt sich ein größerer Anpassungsbedarf. Dieser begründet sich jedoch nicht in den Regelungen der DS-GVO, sondern in Versäumnissen der Vergangenheit.

Vereine tun sich nach wie vor schwer damit, die Anforderungen des Datenschutzes zu erfüllen. Ein wichtiger Grund dafür ist die zum Teil fehlende Akzeptanz dieser Anforderungen. Häufig gehen meine Anrufer pauschal davon aus, dass die Anforderungen von den ehrenamtlich tätigen Personen in den Vereinen nicht vollständig erfüllbar seien. Diese Anforderungen sind aber, wie andere Gesetze auch – beispielhaft sei die Straßenverkehrsordnung, der Umweltschutz und das Vereinsrecht genannt –, von allen Mitgliedern einer Gemeinschaft zu erfüllen. Als europäisches Recht unterliegen sie auch nicht der Dispositionsbefugnis der Nationalstaaten. Gleichwohl gehe ich hier

mit Augenmaß vor und stelle keine übertriebenen Anforderungen, vor allem nicht in zeitlicher Hinsicht. Zusätzlich stehe ich auch beratend zur Verfügung.

Da letztlich die Anforderungen der DS-GVO von allen Vereinen zu erfüllen sind und hierfür zunächst der Vorstand verantwortlich ist, rate ich allen Vereinen zur Benennung einer oder eines Datenschutzbeauftragten. Dies gilt auch dann, wenn keine gesetzliche Pflicht zur Bestellung besteht. Mindestens sollte jeder Verein eine Person bestimmen, die sich des Themas Datenschutz annimmt.

Die Vereine haben mich mit Anfragen im letzten Berichtszeitraum stark belastet. Viele dieser Anfragen befinden sich noch immer in Bearbeitung. Allerdings werden immer mehr Broschüren für Vereine veröffentlicht, aus denen sich Antworten auf die meisten und typischsten Fragen ergeben.

4.8
Inkasso, Auskunfteien

4.8.1
Zulässigkeit der Übermittlung personenbezogener Daten durch die Kreditwirtschaft an Auskunfteien

Für die Übermittlung personenbezogener Daten an Auskunfteien durch Kreditinstitute ist in der Regel keine Einwilligung der Betroffenen erforderlich.

Im Berichtszeitraum haben sich viele Betroffene mit der Frage an mich gewandt, ob ihre Kreditinstitute Daten an Auskunfteien übermitteln dürften, auch wenn sie die von den Banken und Sparkassen vorgelegten „Einwilligungserklärungen“ nicht unterschreiben würden.

Wie sich bei Prüfung der Sachverhalte herausstellte, handelte es sich bei sogenannten „Einwilligungserklärungen“ in allen Fällen um Informationsschreiben, mit denen die Betroffenen darüber informiert wurden, dass die Kreditinstitute personenbezogene Daten wie den Abschluss von Girokonto-, Kredit- oder Kreditkartenverträgen an Auskunfteien übermitteln würden. In keinem Fall handelte es sich tatsächlich um Einwilligungserklärungen.

Leider musste ich feststellen, dass in einigen Fällen seitens einzelner Berater/-innen gegenüber ihren Kund/-innen der Eindruck erweckt wurde, dass die Unterschrift dieser Informationsschreiben zur Fortführung der Geschäftsbeziehung erforderlich sei.

Bei einem hier beispielhaft beschriebenen Formular mit der Bezeichnung „Übermittlung von Daten an die SCHUFA und Befreiung vom Bankgeheimnis“ handelt es sich lediglich um ein Informationsschreiben, das die Bank ihren

Kund/-innen zur Erfüllung der Pflichten nach Art. 13 DS-GVO zur Verfügung stellen muss.

Die Bank teilt darin mit, auf welche Rechtsgrundlage die Übermittlung der Daten an die Auskunftei gestützt wird.

Die Kund/-innen werden in dem Schreiben gebeten, die Aushändigung der Informationen an die/den Kund/-in zu bestätigen. Dies erfolgt lediglich zum Nachweis der Erfüllung der Anforderungen nach Art. 13 DS-GVO. Somit wurde, entgegen anderslautender Äußerungen der Bankmitarbeiter/-innen, keine Einwilligung in die Datenübermittlung erteilt. Auch ist das Unterschreiben einer Ausfertigung des Schreibens datenschutzrechtlich nicht gefordert.

Inhaltlich ist das Dokument hingegen nicht zu beanstanden. Die Bank nennt die korrekten Rechtsgrundlagen, auf die eine Übermittlung ihrer Daten an die Auskunftei gestützt werden kann. Insofern kommt die Bank durch die Aushändigung dieses Informationsblatts den vorgenannten Informationspflichten nach und kann dies nach Unterzeichnung durch die Kunden auch nachweisen. Erforderlich für die Datenverarbeitung ist die Unterzeichnung jedoch nicht.

Die Rechtsgrundlagen, auf welche die Bank die Übermittlung personenbezogener Daten an Auskunfteien stützen kann, sind die Regelungen des Art. 6 Abs. 1 lit. f DS-GVO.

Art. 6 Abs. 1 DS-GVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

So besteht beispielsweise vor Abschluss eines Kreditkartenvertrags während einer aktiven Geschäftsbeziehung seitens der Bank ein berechtigtes Interesse zu erfahren, ob die/der Kreditnehmer/-in bereits andere Verbindlichkeiten hat und/oder ob und wie diese ggf. zurückgeführt worden sind. Mithin darf die Bank Daten bei der Auskunftei erheben und entsprechend den Abschluss eines derartigen Vertrags dann auch an diese übermitteln.

Dieses Vorgehen wird daher von meiner Behörde datenschutzrechtlich nicht beanstandet.

4.8.2
Die Umsetzung des „Code of Conduct“ im Bereich der Auskunfteien

Nach Inkrafttreten der DS-GVO konkretisieren die „Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien“ (Code of Conduct) im Rahmen einer freiwilligen Selbstverpflichtung gemäß Art. 40 DS-GVO die gesetzlichen Regelungen zu den Prüf- und Löschfristen im Bereich der Auskunfteien.

Gegenstand einer Vielzahl an eingehenden Beschwerden ist die Löschung von Einträgen zu Forderungen im Datenbestand von Auskunfteien. Durch das Inkrafttreten der DS-GVO ist jedoch die ehemals in § 35 Abs. 2 Satz 2 Nr. 4 BDSG a. F. enthaltene Prüf- und Löschfrist zu Forderungen weggefallen.

Auskunfteien mussten bis einschließlich zum 24.05.2018 gemäß § 35 Abs. 2 Satz 2 Nr. 4 BDSG a. F. die von ihnen gespeicherten Daten bei erledigten Sachverhalten am Ende des dritten Kalenderjahres bzw. bei nicht erledigten Sachverhalten am Ende des vierten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgte, daraufhin überprüfen, ob eine länger währende Speicherung noch erforderlich war. Das Ergebnis dieser Prüfung konnte dabei von verschiedenen Faktoren abhängen und musste, selbst bei erledigten Forderungen, nicht in jedem Fall die umgehende Löschung der Forderung zur Folge haben. So war beispielsweise eine länger währende Speicherung zulässig, wenn Informationen über Zahlungsstörungen in der Vergangenheit auch nach deren Erledigung noch eine erhebliche Aussagekraft über die Bonität des Betroffenen haben konnten.

Mit Datum vom 25.05.2018 ist der „Code of Conduct“ des Verbandes „Die Wirtschaftsauskunfteien e. V.“, der die Interessen der großen deutschen Wirtschaftsauskunfteien vertritt, durch die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) genehmigt worden. Bei dem „Code of Conduct“ handelt es sich um Verhaltensregeln, die im Rahmen einer freiwilligen Selbstverpflichtung gemäß Art. 40 DS-GVO die

gesetzlichen Regelungen nicht ersetzen, sondern für den Bereich der Wirtschaftsauskunfteien konkretisieren. Der Genehmigung durch die LDI NRW ging ein Beschluss der Datenschutzkonferenz voraus, sodass sichergestellt ist, dass die Genehmigung durch sämtliche deutsche Datenschutzaufsichtsbehörden mitgetragen wird.

Aufgrund vieler Beschwerden im Hinblick auf die Speicherung von Forderungsdaten sind in der Praxis die unter Ziffer II Nr. 1a) und b) des „Code of Conduct" getroffenen Bestimmungen von Bedeutung. Der „Code of Conduct" regelt unter Ziffer II Nr. 1a), dass personenbezogene Daten über fällige und unbestrittene Forderungen gespeichert bleiben, so lange deren Ausgleich nicht bekanntgegeben wurde. Die Notwendigkeit der fortwährenden Speicherung wird jeweils drei Jahre taggenau nach dem jeweiligen Ereigniseintritt überprüft. Gemäß Ziffer II Nr. 1b) des „Code of Conduct" erfolgt eine Löschung der personenbezogenen Daten sodann taggenau drei Jahre nach Ausgleich einer Forderung.

Im Ergebnis lässt sich feststellen, dass der „Code of Conduct" insbesondere durch seinen Bezug auf eine taggenaue Löschung die Rechtsanwendung vereinfacht, die Speicherdauer verkürzt und zur Transparenz bezüglich der Prüf- und Löschfristen beiträgt. So werden im Rahmen der freiwilligen Selbstverpflichtung klar definierte Standards geschaffen, die im Bereich der Auskunfteien eine einheitliche Anwendung der DS-GVO gewährleisten.

4.9
Internet

4.9.1
Veröffentlichung von Beschäftigtenfotos

Bei der Veröffentlichung von Beschäftigtenfotos wird eine schriftliche Einwilligung der betroffenen Mitarbeiter/-innen im Sinne des § 26 Abs. 2 BDSG erforderlich sein. Die Möglichkeit des Widerrufs der Einwilligung gemäß Art. 7 Abs. 3 DS-GVO ist zu beachten.

Im Berichtsjahr haben mich zahlreiche Anfragen dazu erreicht, wie künftig datenschutzkonform mit der Veröffentlichung von Fotos von Beschäftigten umzugehen ist. Bislang war hier das Kunsturhebergesetz (KUG) anzuwenden, das nach der Subsidiaritätsklausel des § 1 Abs. 3 BDSG a. F. als bereichsspezifische Regelung Vorrang hatte.

Seit dem 25.05.2018 gilt die Datenschutzgrundverordnung (DS-GVO), die als europarechtliche Verordnung Anwendungsvorrang vor nationalem Recht genießt. Damit wird die Frage nach der Anwendbarkeit des KUG neu diskutiert.

Art. 88 DS-GVO enthält eine Öffnungsklausel für die Datenverarbeitung im Beschäftigtenkontext, aufgrund welcher nationale Gesetzgeber spezifischere Vorschriften erlassen können. Der deutsche Gesetzgeber hat von diesem Recht Gebrauch gemacht und in § 26 BDSG die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses geregelt, ohne jedoch spezifisch auf das Thema der Veröffentlichung von Beschäftigtenfotos einzugehen.

Rechtsgrundlagen für die Verarbeitung von Beschäftigtenfotos

§ 26 Abs. 1 BDSG

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

§ 26 Abs. 1 BDSG – Erforderlichkeit

§ 26 Abs. 1 BDSG verlangt, dass die Datenverarbeitung zur Durchführung des Beschäftigungsverhältnisses „erforderlich“ ist. Erforderlichkeit bedeutet, dass die berechtigten und schützenswerten Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht der/des Beschäftigten zu einem schonenden Ausgleich zu bringen sind, der beide Interessen möglichst weitgehend berücksichtigt. Notwendig ist somit eine Interessenabwägung zwischen den Belangen der/des Beschäftigten und der verantwortlichen Stelle im Sinne einer Verhältnismäßigkeitsprüfung.

§ 26 Abs. 1 Satz 1 BDSG kommt danach als Rechtsgrundlage nur für den Fall in Betracht, dass die visuelle Präsentation des/der Beschäftigten Gegenstand des Arbeitsvertrages wäre, wie zum Beispiel bei einem Fotomodell. Sollen jedoch „normale“ Mitarbeiter/-innen bei der öffentlichen Darstellung des Unternehmens in Form von Bildern oder Filmsequenzen mitwirken, ist dies zur Durchführung des Beschäftigungsverhältnisses regelmäßig nicht erforderlich, da es überwiegend werblichen Zwecken dient.

§ 26 Abs. 2 BDSG – Einwilligung

§ 26 Abs. 2 BDSG

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

Gem. § 26 Abs. 2 BDSG kann die Rechtmäßigkeit der Verarbeitung auf eine transparente und umfassende Einwilligung der/des Beschäftigten gestützt werden. Die Vorschrift regelt die Bedingungen für die Einwilligung im Beschäftigtenbereich auf der Grundlage von Art. 88 DS-GVO spezifisch. Zu beachten sind als Verlaufsnormen Art. 6 Abs. 1 lit. a DS-GVO und Art. 7 DS-GVO.

Art. 6 Abs. 1 DS-GVO

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben

Art. 7 DS-GVO

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Danach muss die Einwilligung vor der Veröffentlichung und informiert erfolgen, das heißt, die einzelnen Verwendungszwecke sind genau zu bezeichnen, auch die Darstellungsweise des Bildes ist zu regeln.

Große Bedeutung für die Wirksamkeit einer erteilten Einwilligung kommt dem Kriterium der Freiwilligkeit zu. Diese kann insbesondere dann angenommen werden, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen". Über diese vom Gesetz explizit genannten Situationen hinaus ist auch dann regelmäßig von einer freiwilligen Entscheidung der Mitarbeiter/-innen auszugehen, wenn diese eine echte Wahl haben. Dies wäre z. B. dann anzunehmen, wenn Mitarbeiter/-innen die Veröffentlichung ihrer Fotos auch ablehnen können, ohne hieraus Nachteile befürchten zu müssen. Gemäß § 26 Abs. 2 Satz 3 BDSG bedarf die Einwilligung grundsätzlich der Schriftform. § 26 Abs. 2 Satz 4 BDSG verlangt, dass Betroffene die Tragweite ihrer Entscheidung abschätzen können.

Hervorzuheben ist Art. 7 Abs. 3 DS-GVO, wonach Betroffenen ein explizites und jederzeitiges Widerrufsrecht eingeräumt wird, auf das vor Abgabe der Einwilligung hinzuweisen ist. Da dies unter Umständen zu Problemen führen kann, wird empfohlen, die Frage der Löschungspflicht bereits bei Erteilung der Einwilligung zu regeln.

Eingaben, die meiner Behörde vorliegen, betreffen bislang regelmäßig den Sachverhalt, dass eine Mitarbeiterin/ein Mitarbeiter aus dem Unternehmen ausgeschieden ist, ihr/sein Bild aber weiterhin auf der Webseite des Unternehmens veröffentlicht ist. Sofern die Veröffentlichung auf § 26 Abs. 1 Satz 1 BDSG gestützt war, fällt mit Ausscheiden des/der Beschäftigten der Zweck zur Veröffentlichung weg, mit der Folge, dass Art. 17 Abs. 1 lit. a DS-GVO greift: „Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig."

Problematischer ist der Fall, dass eine beschäftigte Person ihre bereits rechtmäßig erteilte Einwilligung in die Veröffentlichung ihres Bildes widerruft und der Arbeitgeber eine möglicherweise kostenintensive Werbekampagne stoppen/löschen muss.

Vor Anwendung der DS-GVO wäre nach Rechtsprechung des Bundesarbeitsgerichts (BAG Urteil vom 11.12.2014 – 8 AZR 1010/13) das KUG zur Anwendung gelangt. Hiernach war im Falle des Widerrufs der Einwilligung in die Veröffentlichung von Bildmaterial eine Gesamtabwägung vorzunehmen und zu verlangen, dass die/der Arbeitnehmer/-in einen Grund angibt, warum er/sie nunmehr ihr/sein Recht auf informationelle Selbstbestimmung gegenläufig ausüben will.

In dem Fall des BAG ging es um ein Firmenvideo, dass reinen Illustrationszwecken diente. Wesentlich war nach Auffassung des BAG insbesondere die Eingriffsintensität in das Persönlichkeitsrecht der/des (ehemaligen) Beschäftigten: Hatte das Bild nur illustrierenden Charakter und wies es kaum einen Bezug zur Persönlichkeit der/des Betroffenen auf, konnte die/der Beschäftigte die Löschung nicht verlangen. Zu berücksichtigen war auch die Verknüpfung des Bildes mit weiteren Informationen über die/den Beschäftigten. Wird etwa durch einen Text die Identität der Mitarbeiterin oder des Mitarbeiters hervorgehoben, ihr/sein Name genannt oder gerade mit ihrer/seiner Zugehörigkeit zum Unternehmen geworben, obgleich sie/er bereits ausgeschieden ist, besteht jedenfalls ein Rechtsanspruch auf Löschung.

Ich bin der Auffassung, dass diese Wertungen des BAG auch unter der Anwendung der DS-GVO und dem neuen BDSG fortgelten, sodass die beschäftigte Person weiterhin den Widerruf der Einwilligung begründen muss und dann die oben erwähnte Interessenabwägung vorzunehmen wäre.

Gestützt werden kann diese Rechtsauffassung u. a. auf die Grundsätze von Treu und Glauben und arbeitsrechtliche Rücksichtnahmepflichten.

Da das bestehende Widerrufsrecht nur ab dem Widerruf Wirkung entfaltet und daher eine einmal erfolgte Veröffentlichung eines Fotos nicht ungeschehen gemacht werden kann und darüber hinaus nicht immer dazu führt, dass die Veröffentlichung für die Zukunft unterbunden wird, sollte über die genauen Bedingungen bereits im Rahmen der Erteilung der Einwilligung informiert werden.

4.9.2
Datensparsamkeit durch die DS-GVO: Radikale Änderungen der DENIC e. G. bei der Registrierung deutscher Domains und bei Whois-Auskünften

Die DENIC e. G. hat zum Wirksamwerden der DS-GVO am 25.05.2018 den Registrierungsprozess für DE-Domains vollständig umgestaltet. Radikale Veränderungen wurden auch am sog. „Whois-Dienst“ vorgenommen, der zuvor eine nahezu unbeschränkte Abfrage der Daten von Domain-Inhabern und für die Domain verantwortlichen Personen ermöglichte. Diese Abfragemöglichkeiten wurden von der DENIC e. G. im Sinne einer nachhaltigen Datenminimierung und -vermeidung erheblich eingeschränkt. In den Umgestaltungsprozess war meine Behörde beratend einbezogen.

Die DENIC e. G. in Frankfurt am Main ist die zentrale deutsche Vergabe- und Registrierungsstelle für Internet-Domains unterhalb der „country code

Top Level Domain“ (ccTLD – länderspezifische Top Level Domain) „.DE“, wie z. B. „hessen.de“ oder „datenschutz.de“. Die DENIC e. G. betreibt im Rahmen des Domain Name Systems (DNS) den Primary-Nameserver für alle aktuell über 16 Millionen Internet-Domains mit der Domain-Endung „DE“. Das hierarchisch aufgebaute DNS-System sorgt dafür, dass weltweit jede Internet-Adresse einmalig und eindeutig adressierbar ist, was die Basis jedes Internet-Angebotes und jeder Internet-Nutzung ist. Mitglieder der DENIC e. G. sind Internet Service Provider (Registrare), die ihren Kunden unter anderem auch die Registrierung einer eigenen DE-Domain bei der DENIC e. G. und oftmals auch den Speicherplatz für eine entsprechende Homepage im World Wide Web (WWW/Internet) auf den Provider-Rechnern und weitere damit zusammenhängende Leistungen anbieten. Die Registrierung der gewünschten Domain der oft auch privaten Endkunden bei der DENIC e. G. erfolgt über diese Internet Service Provider (Registrare).

Für die Registrierung einer Domain verlangte die DENIC e. G. bislang neben den erforderlichen technischen Daten immer auch die Angabe von Name und Anschrift der antragstellenden Person/Organisation (Domain-Inhaber) sowie die entsprechenden Angaben zum administrativen Ansprechpartner (als rechtlich für die Domain verantwortliche Person mit Wohnsitz in Deutschland und Adressat für Rückfragen) und zu den technischen Ansprechpartnern.

Die Daten zum Domain-Inhaber und zur Person des administrativen Ansprechpartners wurden in der Whois-Datenbank der DENIC e. G. gespeichert und waren bis vor dem Wirksamwerden der DS-GVO über den Whois-Dienst auf den Internet-Seiten der DENIC e. G. unbeschränkt weltweit abrufbar. Die tägliche Zahl der Abrufe von Whois-Daten durch Dritte lag bei der DENIC bei ca. 12.000. Jeden Monat wurden also über 360.000 Mal die Daten von DE-Domain-Inhabern und die personenbezogenen Daten von administrativen Ansprechpartnern von DE-Domains über den Whois-Dienst der DENIC e. G. im WWW abgefragt und an die Nutzer des Whois-Dienstes der DENIC e. G. übermittelt. Zu welchen Zwecken diese Abfragen jeweils vorgenommen wurden, blieb unbekannt, da – wie bis dahin weltweit bei allen Whois-Diensten der Domain-Vergabestellen üblich – weder eine Identifizierung oder Authentifizierung noch die Angabe eines berechtigten Interesses der Abfrager vorgenommen wurde.

Dies führte in den letzten Jahren bei meiner Dienststelle immer wieder zu Eingaben betroffener Domain-Inhaber und administrativer Ansprechpartner, in denen die Betroffenen die Veröffentlichung ihrer Daten kritisierten, da sie deren Missbrauch befürchteten oder aus anderen Gründen ein Geheimhaltungsbedürfnis geltend machten (vgl. auch die Vorlage der Landesregierung betreffend den Dreizehnten Bericht der Landesregierung über die Tätigkeit

der für den Datenschutz im nicht-öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden; LTDrucks. 15/1539 vom 30.08.2000, Nr. 9.2 und 9.3). Da für die Domain-Inhaber bzw. die administrativen Ansprechpartner als direkte Vertragspartner der DENIC e. G. allerdings als Vertragsbestandteil (vgl. § 28 Abs. 1 BDSG alt) auch die dortigen Domain-Richtlinien und die Domain-Bedingungen galten, in denen die international übliche Veröffentlichung der Daten über den Whois-Dienst vorgesehen war, konnte den Beschwerden durch meine Behörde nicht abgeholfen werden. Ein Recht auf eine anonyme Domain-Registrierung lässt sich aus dem Datenschutzrecht jedenfalls nicht ableiten. Den Betroffenen wurde daher regelmäßig von meiner Behörde empfohlen, einen Vertretungsberechtigten wie z. B. einen Rechtsanwalt bei der DENIC e. G. eintragen zu lassen, damit anstelle der eigenen Daten dessen Daten über den Whois-Dienst abgerufen werden könnten.

Bei der DENIC e. G. wurde allerdings immer sehr genau beobachtet, wie sich in den letzten Jahren die kritische Diskussion über den Whois-Dienst auf europäischer Ebene entwickelte und welche Anstrengungen insbesondere die europäischen Datenschutzbehörden über die sog. Artikel 29-Datenschutzgruppe gegenüber der ICANN („Internet Corporation for Assigned Names and Numbers“, diese koordiniert die Vergabe von einmaligen Namen und Adressen im Internet, organisiert das „Domain Name System“ und die entsprechende Zuteilung von IP-Adressen, regelt auch den Whois-Dienst) unternahm, um künftig die bislang nahezu unbegrenzte Veröffentlichung personenbezogener Daten von Domain-Inhabern und administrativen Ansprechpartnern von Domains zu verhindern oder zumindest effektiv zu beschränken. Für die DENIC e. G. war absehbar, dass auch der Europäische Datenschutzausschuss (European Data Protection Board, EDPB) als Nachfolgegremium der Artikel 29-Datenschutzgruppe diese Bemühungen zur Beschneidung des Whois-Dienstes unter den aus Datenschutzsicht verbesserten Rahmenbedingungen der DS-GVO fortsetzen würde. Unter dem Eindruck dieser Diskussion auf internationaler Ebene und vor dem Hintergrund der bevorstehenden Neuregelung des europäischen Datenschutzrechts durch die DS-GVO zum 25.05.2018 entschloss sich die DENIC e. G., ihre Datenerhebung und -verarbeitung im Zusammenhang mit der Registrierung von DE-Domains ab diesem Termin erheblich datensparsamer zu gestalten. Auch der Whois-Dienst der DENIC e. G. wurde zum Zeitpunkt des Wirksamwerdens der DS-GVO so abgeändert, dass nun wesentlich weniger Daten bei Domain-Abfragen an deutlich weniger Abfrager in einem neuen, abgestuften Verfahren an berechtigte Stellen übermittelt werden. Diese Veränderungen wurden mir zur datenschutzrechtlichen Beurteilung vorgestellt; die DENIC e. G. wurde hierzu intensiv beraten.

Seit dem Wirksamwerden der DS-GVO zum 25.05.2018 werden von den Providern (Registrare) neben den notwendigen technischen Daten an die DENIC e. G. nur noch die Daten des Domain-Inhabers weitergegeben. Dieser Domain-Inhaber kann eine natürliche oder juristische Person sein und seinen Sitz auch im Ausland haben. Daten zum administrativen Ansprechpartner (immer eine natürliche Person) sowie zum technischen Verantwortlichen und zum Zonenverantwortlichen werden von der DENIC e. G. nun nicht mehr benötigt, liegen dort nicht mehr vor und können auch nicht mehr bei der DENIC e. G. abgefragt werden.

Der Provider (Registrar), über den eine Domain beantragt wird, stellt zusätzlich zu jeder Domain zwei nicht personalisierte E-Mail-Adressen zur Verfügung, die dann bei einer Whois-Abfrage zu der jeweiligen Domain veröffentlicht werden. Eine der E-Mail-Adressen soll für Beschwerden gegen die Domain oder den Inhaber genutzt werden (Abuse-Request), die andere E-Mail-Adresse für alle anderen Kontaktzwecke (General-Request). Die Herausgabe der Daten von Domain-Inhabern und administrativen Ansprechpartnern von Domains erfolgt in diesen Fällen also gänzlich ohne Zutun der DENIC e. G. ausschließlich über den Provider (Registrar) über die von diesem bereitgestellten E-Mail-Adressen. Die DENIC e. G. veröffentlicht bei einer Whois-Abfrage neben den beiden E-Mail-Adressen nur noch den Domain-Status (registriert oder nicht registriert) und einige rein technische Daten zur angefragten Domain.

Für die rechtlich unproblematischen Whois-Abfragen durch den Domain-Inhaber selbst (zur Kontrolle seiner Daten) und durch andere DENIC-Mitglieder (für den Fall des beabsichtigten Provider-Wechsels) wurden meiner Behörde geeignete Verfahren vorgestellt:

Bei Abfragen durch den Domain-Inhaber selbst muss die bei der Domain-Registrierung angegebene E-Mail-Adresse und die Postleitzahl angegeben werden. Das Abfrageergebnis wird dem Abfrager über einen zeitlich begrenzt gültigen Link präsentiert, der per E-Mail an die hinterlegte bzw. angegebene E-Mail-Adresse des Domain-Inhabers gesendet wird. Für den Zweck des Providerwechsels wird ein zusätzliches Passwort eingeführt, das angegeben werden muss, wenn ein Provider (Registrar, DENIC-Mitglied) aus diesem Grund die Inhaberdaten erfahren möchte.

Für anders begründete Whois-Abfragen werden nun verschiedene PDF-Anträge für Inhaber-Auskünfte angeboten, damit die DENIC e. G. vor der Datenübermittlung jeweils prüfen kann, ob ein berechtigtes Interesse auf Seiten des Anfragers vorliegt, auf das eine Datenübermittlung an diesen gestützt werden kann. Die ausgefüllten Anträge werden von der DENIC e. G. nach Eingang (Briefpost, Telefax) manuell überprüft und beurteilt. Danach erteilt die DENIC e. G. Domain-Inhaberauskünfte bei Vorliegen entsprechender

berechtigter Interessen oder belastbarer Rechtsgrundlagen auf begründeten Antrag nur noch an folgende Stellen:

1. Behörden im Rahmen ihrer hoheitlichen Tätigkeit (etwa im Bereich der Strafverfolgung, Gefahrenabwehr oder Pfändungsverfügung),
2. Inhaber eines Namens- oder Kennzeichenrechts, das durch die Domain möglicherweise verletzt wird,
3. Anspruchsteller, die im Besitz eines vollstreckbaren Titels sind und die zivilrechtliche Pfändung der domainvertraglichen Ansprüche des Domain-Inhabers beabsichtigen, und
4. Insolvenzverwalter über das Vermögen eines (auch mutmaßlichen) Domain-Inhabers.

In allen anderen Fällen erteilt die DENIC e.G in der Regel keine Auskünfte mehr. Dennoch ist nach meiner Auffassung grundsätzlich weiterhin gewährleistet, dass beim Vorliegen geeigneter Rechtsgrundlagen von der DENIC e. G. und bei sonstigen Rechtsverletzungen durch eine Webseite von dem Provider über die bereitgestellte Abuse-Adresse die Daten der Domain-Verantwortlichen herausgegeben werden, damit Rechtsansprüche korrekt adressiert und durchgesetzt werden können.

Mir wurden die entsprechenden Antragsformulare zur Beratung und datenschutzrechtlichen Stellungnahme vorgelegt. Das neue Verfahren bei der Domain-Registrierung und insbesondere die Einschränkungen des Whois-Dienstes bezüglich der abfragefähigen Daten und der abfrageberechtigten Stellen wurden von mir ausdrücklich begrüßt. Die Erhebung und Verarbeitung personenbezogener Daten durch die DENIC e. G. orientiert sich heute an den Prinzipien der Datenvermeidung und der Datensparsamkeit. Die DENIC e. G. praktiziert hier vorbildlich den Datenschutz durch Technikgestaltung i. S. v. Art. 25 DS-GVO und Erwägungsgrund 78 (privacy by design).

Die ersten Monate mit dem neuen Whois-System haben zudem gezeigt, dass sich die Anzahl der per Antrag gestellten Whois-Abfragen durchaus in Grenzen hält und dass eine manuelle Bearbeitung die DENIC e. G. nicht überfordert. Während früher täglich ca. 12.000 Whois-Abfragen durch Dritte über das Internet vorgenommen wurden, hat sich die Zahl der Abfragen durch berechtigte Dritte (Behörden, Inhaber von Namens- oder Kennzeichenrechten, Inhaber von vollstreckbaren Titeln und Insolvenzverwalter) auf ca. 40 pro Tag reduziert. Durch das neue Whois-Verfahren werden im Vergleich mit dem vorherigen Verfahren also täglich über 11.000 Übermittlungen personenbezogener Daten an Dritte vermieden. Dies kann meines Erachtens mit Fug und Recht als großer Erfolg und eine beispielhafte Umsetzung der DS-GVO durch die deutsche Domain-Vergabestelle DENIC e. G. gewertet werden.

4.10
Technik, Organisation

4.10.1
Standard-Datenschutzmodell wird konkret: Wenden Sie DS-GVO-konforme Maßnahmen an

Aus der Sicht der Informationstechnik gibt es einen Reigen von Artikeln in der Datenschutzgrundverordnung (DS-GVO), die das Ergreifen und das Vorhalten geeigneter Maßnahmen erforderlich machen, sodass dauerhaft eine datenschutzkonforme Verarbeitung personenbezogener Daten erfolgt. Mindestens den folgenden Artikeln ist inhärent, dass Verantwortliche und Auftragsverarbeiter zu entscheiden haben, was in der Informationstechnik getan werden muss und wie IT-Systeme in eine Unternehmens- oder Organisationsstruktur eingebettet werden sollen: Art. 13 bis Art. 22, Art. 25, Art. 30, Art. 32, Art. 35 i. V. m. Art. 36 DS-GVO. In jedem Fall sind technische und organisatorische Maßnahmen (TOMs) zu ergreifen. Mit dem Standard-Datenschutzmodell (SDM) und seinen Bausteinen in einem fortzuschreibenden Maßnahmenkatalog ist begonnen worden, diverse solche Anleitungen zu veröffentlichen.

Standard-Datenschutzmodelle und Bausteine im Maßnahmenkatalog

Mit dem Standard-Datenschutzmodell (SDM) wird eine Methode bereitgestellt, mit der Verantwortliche und Aufsichtsbehörden bei der Entwicklung, bei der Datenschutzberatung und bei der Prüfung von Datenverarbeitungen beurteilen können, ob personenbezogene Daten datenschutzkonform nach DS-GVO verarbeitet werden. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat empfohlen, dieses Modell zur Erprobung anzuwenden. Das Handbuch zum Standard-Datenschutzmodell in der Erprobungsfassung (Version 1.1) steht zum Download unter https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V_1_1.pdf bereit (letzter Aufruf: 19.11.2018). Durch den AK Technik werden diese und weitere in diesem Beitrag genannten Quellen bereitgestellt und gepflegt. Der entsprechende Einstieg findet sich unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

Handbuch zum Standard-Datenschutzmodell ist ein Rahmenwerk, das durch konkrete zu ergreifende Maßnahmen zu ergänzen ist, um die Anforderungen der DS-GVO aus Sicht der Informationstechnik noch besser zu unterstützen. Zu solchen Maßnahmen wird es jeweils einen sogenannten Baustein geben. Die ersten Bausteine sind verfügbar und werden in der Pressemitteilung vom 10.09.2019 unter https://datenschutz.hessen.de/pressemitteilungen/pressemitteilung-zum-standard-datenschutzmodell (letzter Aufruf: 19.11.2018)

erläutert. Diese sieben Bausteine beziehen sich – angeführt in alphabetischer Reihenfolge – auf Aufbewahrung, Datenschutzmanagement, Dokumentation, Löschen und Vernichten, Planung, Protokollierung und Trennung.

Technischer Datenschutz: Gewährleistungsziele

Sowohl das SDM-Handbuch als auch die jeweiligen Bausteine zur Ausgestaltung technischer und organisatorischer Maßnahmen ziehen zur Bewertung Ziele des technischen Datenschutzes – die Gewährleistungsziele – heran. Die Gewährleistungsziele sind Integrität, Vertraulichkeit, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit. In jedem Baustein des Maßnahmenkatalogs wird erläutert, welches Gewährleistungsziel mit Anwendung der entsprechend beschriebenen technischen und organisatorischen Maßnahmen umgesetzt werden kann.

Bausteine

Die im Folgenden beschriebenen Bausteine wurden von Aufsichtsbehörden aus Hessen, Mecklenburg-Vorpommern, Sachsen und Schleswig-Holstein sowie von der Evangelischen Kirche Deutschlands erarbeitet und veröffentlicht. Sie sind keine Publikation der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Bei den sich immer noch verkürzenden Innovationszyklen in der IT-Einwicklung ist es erforderlich, den Verantwortlichen und Auftragsverarbeitern, speziell den jeweiligen IT-Abteilungen Empfehlungen auszusprechen. Die Erprobung der folgenden Bausteine ist zu begrüßen, mit denen Verarbeitungen DS-GVO-konformer gestaltet werden können. Die Nennung der veröffentlichten Bausteine erfolgt in alphabetischer Reihenfolge – bis auf den Baustein Datenschutzmanagement, in dem grundlegende Aspekte der Verwaltung und der dauerhaften, stetig zu evaluierenden Umsetzung datenschutzrechtlicher Anforderungen betrachtet werden.

<u>Baustein: Aufbewahrung</u>

Personenbezogene Daten müssen aufbewahrt werden. Sie sind vom Zeitpunkt der Erhebung über die gesamte Dauer der rechtlich gebotenen Speicherfristen bis zum Zeitpunkt der Aussonderung (Abgabe an Archive, Löschung und Vernichtung) zur Verarbeitung bereitzuhalten. Daher umfasst die Speicherung das Erfassen, das Aufheben und Aufbewahren personenbezogener Daten. Der Baustein beschreibt technische und organisatorische Maßnahmen zur Speicherung personenbezogener Daten in elektronischer Form im ope-

rativen Betrieb bzw. im Produktivsystem oder in Papierform. Im Zentrum der Betrachtung stehen die Gewährleistungsziele Verfügbarkeit, Integrität, Intervenierbarkeit und Transparenz.

Für aufzubewahrende Daten wird ein gestuftes Konzept vorgeschlagen, das eine Abwägung zwischen Papierform, Speicherung in operativen IT-Systemen mit ggf. notwendigen Emulations- und Virtualisierungstechniken sowie die Überführung von Datenobjekten in neuere digitale Repräsentationen ermöglicht.

In diesem Baustein wird das Aufbewahren von Daten in Form einer Datensicherung (Back-ups) nicht betrachtet. Zur Klärung datenschutzrechtlicher Anforderungen bzgl. einer Datensicherung wird es zukünftig einen eigenen Baustein im Maßnahmenkatalog geben.

Baustein: Dokumentation

Aus der Sicht des technischen Datenschutzes sind mit einer Dokumentation mehrere Aufgaben zu erfüllen, die im Wesentlichen dem Gewährleistungsziel der Transparenz dienen. Weitere Gewährleistungsziele werden je nach Ausrichtung der Dokumentation ebenso bedient bzw. sind zu berücksichtigen.

Diese Aufgaben werden im Folgenden aufgezählt und in Kürze erläutert:

1. In Hinblick auf den Einsatz von IT-Systemen zur Verarbeitung personenbezogener Daten besteht eine Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO. Der Verantwortliche ist verpflichtet nachzuweisen, dass die datenschutzrechtlichen Anforderungen entsprechend Abs. 1 ebendort eingehalten werden, die jeweils mit mindestens einem datenschutzrechtlichen Terminus abschließen: „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit“. Offensichtlich ist, dass eine Dokumentation der Verarbeitung darstellt, *was* verarbeitet wird und *wie* sie durchgeführt wird, um insbesondere dann ebenso Anforderungen aus dem Art. 30 DS-GVO zu erfüllen.
2. Die Dokumentation dient konkret – auch in Hinblick auf Art. 25 und Art. 32 DS-GVO –
   a. der Gewährleistung der Transparenz von Datenbeständen,
   b. der Darstellung der Transformation von Daten in ein adäquates Modell für die tatsächliche organisatorische und technische Umsetzung einer Verarbeitung,
   c. der Beschreibung der eingesetzten Komponenten und ihrer Funktionalitäten und Schnittstellen,

d. der Festlegung der Prozesse innerhalb von IT-Systemen, Organisationen und über IT-System- und Organisationsgrenzen hinweg sowie
e. der Nachvollziehbarkeit von Entscheidungen und im Verwaltungshandeln.

Die Punkte a und e fokussieren das vorher erwähnte „Was". Punkt c. liefert Informationen über das „Wie". Die Punkte b und d haben verbindenden Charakter. Hier ist die Perspektive entscheidend, ob mehr das „Was" oder mehr das „Wie" betrachtet wird. So ist z. B. aus Organisationssicht die Festlegung der Prozesse ein „Wie", um eine Organisation handlungsfähig zu machen und zu halten. Hingegen ist die gleiche Festlegung aus der Perspektive der IT, die IT-gestützte Prozesse zu implementieren hat, eine Antwort auf die Frage, „was" zu tun ist. Schließlich wird in der Zusammenschau der Punkte a bis e deutlich, dass datenschutzrechtliche Anforderungen immer nur in einem organisations- und fachübergreifenden Team beim Verantwortlichen dauerhaft umsetzbar sind.

3. Aus Gründen der allgemeinen Nachvollziehbarkeit empfiehlt es sich, zur Dokumentation datenschutzrechtlicher Anforderungen strukturelle Festlegungen zu treffen. Solche Festlegungen können sich beziehen auf
   a. die Strukturierung der Gesamtdokumentation,
   b. die Verarbeitung in Papierform oder elektronisch,
   c. die Angemessenheit und den Umfang,
   d. die Vollständigkeit,
   e. die Revisionsfestigkeit,
   f. die notwendige Aktualität und auch
   g. die Fortschreibung der Dokumentation.
4. Darüber hinaus sollte die Dokumentation für die Einhaltung der Rechte betroffener Personen (Art. 12 bis 22 DS-GVO) genutzt werden, um z. B. Verarbeitungsvorgänge in Abhängigkeit von Einsatzgebiet und Anwendungsfall zu konkretisieren.

Neben diesen wesentlichen Aufgaben findet im Baustein eine Differenzierung statt, wenn bei der Verarbeitung ein hohes Risiko für Rechte und Freiheiten betroffener Personen besteht.

Baustein: Planung und Spezifikation

Ziel dieses Bausteins ist es darzustellen, welche Aktivitäten aus der operativen Gestaltung einer Verarbeitungstätigkeit sich in selbstverständlicher Weise mit der Umsetzung datenschutzrechtlicher Anforderungen verknüpfen lassen. So wird Bezug auf ein Vorgehen Verantwortlicher als Auftraggeber

genommen, in dem er plant und erklärt, was und wie durch einen Auftragnehmer, z. B. auch Auftragsverarbeiter, zu leisten ist bzw. in welcher Weise datenschutzrechtliche Anforderungen für eine IT-gestützte Verarbeitung umzusetzen sind.

Im Fokus ist neben der Planung die Spezifikation einer Verarbeitungstätigkeit. Grund hierfür ist, dass eine Spezifikation in vielfacher Weise in der IT Wiederverwendung finden muss, um eine funktionstüchtige IT und qualitativ hochwertige Prozesse auf Dauer zu erhalten, die in gleicher Weise datenschutzrechtliche Anforderungen erfüllen. Wie aus der IT-Entwicklung bekannt, sind dazu regelmäßige Vergleiche auf verschiedenen Ebenen einer Verarbeitungstätigkeit zwischen dem Soll aus der Spezifikation und dem Ist im laufenden Betrieb erforderlich.

Um solche Soll- und Ist-Vergleiche durchführen zu können, sind mindestens erforderlich:

– eine Beschreibung der Verarbeitungstätigkeit, wie sie auch in Art. 30 DS-GVO verlangt ist,
– eine Dokumentation der Rechtsgrundlagen, auf denen die Ausführung der Verarbeitungstätigkeit erfolgt,
– eine Dokumentation des Verantwortlichen und der Beteiligten in einer Organisation oder einem Unternehmen,
– eine Spezifikation fachlicher Prozesse,
– eine Spezifikation der Fachapplikation mit Darstellung typischer Anwendungsfälle im Einsatzgebiet der IT-Systeme und/oder ihrer Komponenten, sodass Beteiligte oder potenziell unbefugte Dritte identifiziert werden können,
– eine in angemessener Form gegebene Beschreibung funktionaler und nicht-funktionaler Anforderungen und ihren Schnittstellen, die in erforderlicher Weise im Zusammenhang mit einer Risikobetrachtung für Rechte und Freiheiten betroffener Personen stehen,
– eine Bestimmung und Dokumentation zu ergreifender bzw. ergriffener technischer und organisatorischer Maßnahmen und
– eine Festlegung zur Administration von technischen Systemen und Programmen unter Nennung der Administratoren selbst, sodass Verfügbarkeit, Vertraulichkeit und Integrität auch unter Belastung für die gesamte Betriebsdauer der Systeme und Programme gewährleistet sind.

Daher dient dieser Baustein der eigenen Kontrolle in der Organisation oder im Unternehmen wie auch der Prüfbarkeit durch die zuständige Datenschutzaufsichtsbehörde. Aus Sicht der Organisationskontrolle steht das

Gewährleistungsziel der Transparenz im Fokus. Hinzu kommen aus Sicht der Informationstechnik

– die Gewährleistung und Prüfbarkeit von Verfügbarkeit, Vertraulichkeit und Integrität sowie
– die Anforderung an die Umsetzung, dass die Verarbeitung auf der Basis von IT-gestützten Prozessen auch unter Belastung gewährleistet sein muss.

Baustein: Protokollierung

Mit einer Protokollierung wird eine bereits ausgeführte Verarbeitung, Verarbeitungstätigkeit oder speziell ein Verarbeitungsvorgang wiedergegeben. Sie dient der Prüfbarkeit einer oder mehrerer Ereignisse, die bereits stattgefunden haben. Dabei ist eine Vergleichbarkeit zwischen vorgesehenen und ausgeführten Aktivitäten herzustellen, die ebenso datenschutzkonform erfolgen müssen. Aus organisatorischer Sicht geht es um die Nachvollziehbarkeit von fachlichen und/oder administrativen Entscheidungen und deren Umsetzung. Aus technischer Sicht sind organisatorische und technische Maßnahmen zu betrachten, mit denen fachliche und/oder administrative Entscheidungen in der IT realisiert werden. Das gilt auch im dauerhaften Betrieb der IT. Hier ist nachzuweisen, dass die jeweilige Protokollierung valide, nachvollziehbar, aktuell und vollständig ist, wobei jede Protokollierung nur zweckgebunden erfolgen darf. Gleichzeitig ist rückbezüglich für Protokolldaten zu gewährleisten, dass festzustellen ist, auf welcher Ebene die Protokollierung erfolgte und wie ggf. die Protokolldaten zusammengehören. Entsprechend ist zu berücksichtigen, dass die Umsetzung der Protokollierung in ihrem Charakter verarbeitungs- und systemübergreifend ist.

Abhängig davon, ob eine verarbeitungs- und/oder systemübergreifende Protokollierung vorliegt, sind zu unterscheiden:

– Nutzeraktivitäten in einer Fachapplikation,
– Systemaktivitäten,
– Administrationstätigkeiten oder auch
– Aktivitäten über Schnittstellen.

Typische Protokolldaten sind bestimmt durch:

– eine Zeitkomponente bzw. einen Zeitpunkt eines zu protokollierenden Ereignisses oder des protokollierten Ereignisses im laufenden Betrieb,
– eine Angabe einer Instanz – i. d. R. mit Bezug zum eingesetzten IT-System –, um festzuhalten, wer hat protokolliert,
– eine Angabe eines Grundes oder eines spezifischen Ereignisses, um festzuhalten, warum protokolliert wurde und

– eine Angabe des Speicherorts, sodass zu ermitteln ist, durch wen und an welcher Stelle protokolliert wurde.

Somit dient der Einsatz der Protokollierung der Umsetzung der Gewährleistungsziele Transparenz und Integrität.

Zudem ist die Zweckbindung zu gewährleisten. Mit Protokolldaten ist besonders sorgsam umzugehen, da in ihnen unter Anwendung von IT-gestützten Auswertungsmechanismen im laufenden Betrieb potenziell eine Überwachung nicht betroffener Personen angelegt ist. Daher darf die Verarbeitung von Protokolldaten nur in wohldefinierten Fristen stattfinden. Entsprechend sind technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO zu ergreifen. Schließlich bedarf es einer entsprechenden dokumentierten Abwägung beim Einsatz einer Protokollierung, u. a. der Verarbeitungsvorgänge für die Protokolldaten gespeichert werden.

Des Weiteren sind Mechanismen zur Aufbereitung von Protokolldaten zu betrachten, zu denen eine Filterung, eine Normalisierung, eine Aggregation, eine Kategorisierung oder eine Priorisierung gehören können. Diverse mögliche Mechanismen zur Protokollierung sind im Baustein ausgeführt.

Baustein: Löschen und Vernichten

Das Löschen beschreibt im allgemeinen Sprachgebrauch das Unzugänglichmachen von Daten und umfasst sowohl reversible und irreversible Prozesse. Im juristischen Sinn ist Löschen das dauerhafte Unkenntlichmachen gespeicherter personenbezogener Daten mittels geeigneter Prozesse. Hier reichen diese Prozesse vom irreversiblen Unzugänglichmachen einzelner personenbezogener Daten bis zur physikalischen Zerstörung eines gesamten Datenträgers (Vernichtung). Der Baustein beschreibt die datenschutzrechtlichen Anforderungen im juristischen Sinn.

Der Baustein dient der Unterstützung der Gewährleistungsziele Vertraulichkeit, Intervenierbarkeit und Nichtverkettung.

Die Pflicht zur Löschung betrifft unter Berücksichtigung verfügbarer Technologien und der Implementierung angemessener Maßnahmen sowohl aktive personenbezogene Daten in Abhängigkeit verarbeitungsspezifischer Löschfristen als auch Sicherheitskopien, Protokolldaten in IT-Systemen und aus verarbeitungstechnischen Gründen temporäre Daten besonders in IT-gestützten Prozessen.

Unterschiedliche Ansätze unter Berücksichtigung von Einsatzgebiet und Anwendungen in der Informationstechnik sind für das Löschen und Vernichten im operationalen Betrieb im Baustein erläutert.

Baustein: Trennung

Aus datenschutzrechtlicher und informationstechnischer Perspektive bedingen verschiedene Zwecke unterschiedliche Befugnisse bzgl. der Verarbeitung personenbezogener Daten. Entsprechend sind zur Durchsetzung der Gewährleistungsziele Nichtverkettung, Integrität und Vertraulichkeit ebenso unterschiedliche Trennungsmaßnahmen durchzusetzen. Die eingesetzte Technik auf der Basis von Daten, IT-Systemen und Prozessen muss sich am genannten Zweck und am Stand der Technik orientieren, entsprechend eingerichtet sein und dauerhaft betrieben werden. Sind eine abgeschlossene Datenhaltung oder unabhängig voneinander zu implementierende Prozesse umzusetzen, dann muss das IT-System mandantenfähig sein.

In diesem Baustein sind sieben Prüfschritte zur Mandantentrennung angeben, die unternehmens- oder organisationsintern durchgeführt werden können. Auf diese Weise kann selbstständig und selbsttätig eingeschätzt werden, ob eine Verarbeitung datenschutzkonform ist. Diese sieben Schritte bestehen aus:

1. einer vorausgehenden rechtlichen Betrachtung, insbesondere unter Hinzunahme von spezialgesetzlichen Bestimmungen,
2. einer Prüfung eines bestehenden Abschottungsgebots,
3. einer Prüfung bzgl. eines organisationsbezogenen Trennungsgebots,
4. einer revisionssicheren Ausgestaltung der Übermittlung personenbezogener Daten zwischen zwei Mandanten,
5. einer Umsetzung abgeschlossener Transaktionen innerhalb eines Mandanten,
6. einer Prüfung unabhängiger Konfigurationen unterschiedlicher Mandanten und
7. einer Beschränkung der mandatenübergreifenden Verwaltung der verarbeiteten personenbezogenen Daten.

Diese sieben Schritte sind im Baustein ausführlicher dargestellt.

Baustein: Datenschutzmanagement

Der Baustein zum Datenschutzmanagement hat anderen Charakter als die bisher dargestellten Bausteine. Das Datenschutzmanagement zielt auf einen kontrollierten, gesteuerten Prozess während des gesamten Lebenszyklus einer oder mehrerer Verarbeitungstätigkeiten, wie sie gemäß Art. 30 DS-GVO zu verwalten sind. Der folgende SDM-basierte Lebenszyklus soll Verantwortliche und Auftragsverarbeiter unterstützen, dass datenschutzrechtliche Anforderungen, insbesondere durch geeignete technische und organisatorische Maßnahmen, spezifiziert, dokumentiert, umgesetzt, dauerhaft nach Stand

der Technik vorgehalten, evaluiert werden und nachgewiesen werden. Der dazugehörige kontinuierliche Verbesserungsprozess lässt sich in folgender Abbildung “Zyklus des Datenschutzmanagements“ darstellen, der eine ständige Beobachtung des laufenden Betriebs ermöglicht.

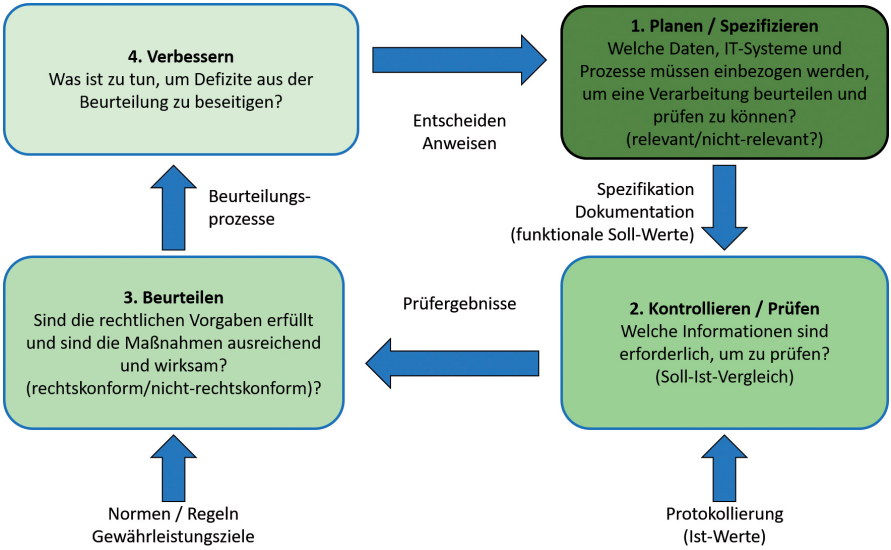


Abbildung: Zyklus des Datenschutzmanagements
(Quelle: Baustein – Datenschutzmanagement, veröffentlicht am 10.09.2018)

Die einzelnen Phasen und hiermit verbundenen notwendigen Aktivitäten werden im Baustein entsprechend erläutert.

Fazit und Ausblick

Dieser Abriss der bisher veröffentlichten Bausteine bietet einen Einblick, in welcher Weise die Umsetzung von datenschutzrechtlichen Anforderungen mit Schwerpunkt auf dem Ergreifen geeigneter technischer und organisatorischer Maßnahmen erfolgen sollte. Verantwortlichen, Auftragsverarbeitern und IT-Leitern ist empfohlen, ihre Erfahrungen bei der Erprobung der Bausteine den an der Entwicklung beteiligten Datenschutzaufsichtsbehörden mitzuteilen; z. B. per Mail an: sdm@datenschutz-mv.de.

Weitere Bausteine sollen in zügiger, wenn auch loser Folge im Jahr 2019 veröffentlicht werden.

4.10.2
MUSS-Listen in Europa zur Durchführung einer Datenschutzfolgenabschätzung

Mit dem Wirksamwerden der Datenschutz-Grundverordnung sind die Datenschutzaufsichtsbehörden verpflichtet, eine Liste gemäß Art. 35 Abs. 4 zu veröffentlichen. In dieser sogenannten MUSS-Liste sind Verarbeitungsvorgänge zu benennen, für die die zuständige Datenschutzaufsichtsbehörde eine Datenschutzfolgenabschätzung als zwingend erforderlich ansieht.

Eine Datenschutzfolgenabschätzung (DSFA) ist vorzunehmen, wenn bei der Durchführung einer Verarbeitung personenbezogener Daten potenziell ein hohes Risiko für Rechte und Freiheiten betroffener Personen besteht. Schon im vorausgegangenen 46. Tätigkeitsbericht für das Jahr 2017 wurden in „2.6 Datenschutz-Folgenabschätzung (DSFA) nach DS-GVO: Was kann durch sie geleistet werden?“ die diesbezüglichen Rahmenbedingungen erläutert (Quelle: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2017_46_TB_0.pdf; letzter Aufruf: 26.11.2018).

Deutsche MUSS-Liste

Durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde eine bundesweit abgestimmte Liste gemäß Art. 35 Abs. 4 DS-GVO in der Unterarbeitsgruppe DSFA (UAG DSFA) des Arbeitskreises Technik (AK Technik) erarbeitet. Meine Mitarbeiterin hat regelmäßig an den Treffen der UAG DSFA teilgenommen. Dabei wurde bewirkt, dass die ursprüngliche Liste um fünf Einträge gekürzt wurde. Eine übersichtliche MUSS-Liste ist zu bevorzugen, da sie für hessische Betriebe, Firmen und Unternehmen handhabbar bleiben muss.

Die Struktur dieser deutschen MUSS-Liste orientiert sich bereits an den Anforderungen einer Leitlinie der Art. 29-Gruppe (heute: Europäischer Datenschutzausschuss; EDSA) mit dem Titel „Guidelines on Data Protection Impact Assessment“ (WP248 rev.01; 13.10.2017; Quelle: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236). Hierin sind neun Verarbeitungsvorgänge genannt, die eine DSFA erforderlich machen können:

– Bewerten oder Einstufen (Scoring)
– automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
– systematische Überwachung
– vertrauliche oder höchstpersönliche Daten

– Datenverarbeitung im großen Umfang
– Abgleichen oder Zusammenführen von Datensätzen
– Daten zu schutzbedürftigen betroffenen Personen
– innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
– Hinderung einer betroffenen Person an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. der Durchführung eines Vertrags

Dabei sind diese Verarbeitungsvorgänge im Zusammenhang mit dem Einsatzgebiet der jeweiligen IT und bzgl. des (Anwendungs-)Kontexts im Sinn einer Verarbeitungstätigkeit gemäß Art. 30 DS-GVO zu betrachten. Solche möglichen Verarbeitungstätigkeiten wurden weiter konkretisiert und um Beispiele ergänzt. Diese MUSS-Liste findet sich mit einem erklärenden hessischen Begleittext unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorgänge-Muss-Liste.pdf (Stand: August 2018 in Version 1.1, letzter Aufruf 26.11.2018). Abgesehen von dem erklärenden Text habe ich mich entschieden, keine Änderungen gegenüber der ursprünglichen, DSK-abgestimmten Version der Liste vorzunehmen, obwohl mir dies möglich gewesen wäre. Aus meiner Sicht sollte diese MUSS-Liste besonders Betrieben, Firmen und Unternehmen im IT-Bereich Klarheit bieten. Das ist besonders wichtig, wenn sie in Deutschland länderübergreifend arbeiten. Andere Datenschutzaufsichtsbehörden der Länder haben individuelle Anpassungen vorgenommen. Die MUSS-Liste ist nicht abschließend. Wenn der Verantwortliche oder der Auftragsverarbeiter ein hohes Risiko für Rechte und Freiheiten betroffener Personen bei der Risikobetrachtung für eine Verarbeitungstätigkeit (Art. 30 DS-GVO) ermittelt, dann hat er in jedem Fall eine DSFA durchzuführen. Zusätzlich kann die zuständige Datenschutzaufsichtsbehörde eine DSFA anfordern.

Einreichung der MUSS-Liste beim Europäischen Datenschutzausschuss

Diese DSK-abgestimmte MUSS-Liste wurde im Rahmen eines Art. 63-Verfahrens, dem Kohärenzverfahren, gemäß Art. 35 Abs. 6 zur Abgabe einer Stellungnahme nach Art. 64 DS-GVO an den EDSA übersandt. Die bis August 2018 von 22 Mitgliedstaaten zur Stellungnahme eingesandten MUSS-Listen wurden durch die Expertengruppe „Technical Subgroup“ für den EDSA in einer Zusammenschau bewertet. Dabei stellte die Expertengruppe fest, dass nur drei Einträge der eingesandten Listen europaweit einer gleichen Einschätzung unterlagen:

– Generische Daten sind wie biometrische Daten zu bewerten; vgl. dazu Art. 9 DS-GVO.
– Gesundheitsdaten müssen einer differenzierten Betrachtung unterliegen und sind somit im Anwendungskontext und der eingesetzten Technologie zu betrachten.
– Die Hervorhebung von Geolokalisationsdaten darf nicht dazu führen, dass jeder kleine oder mittlere Betrieb verpflichtet wird, einen betrieblichen Datenschutzbeauftragten bestellen zu müssen.

Jedem Mitgliedstaat wurde vom EDSA eine spezifische Stellungnahme zugesendet. Diese Stellungnahme des EDSA bzgl. der deutschen MUSS-Liste wurde am 25.09.2018 unter https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_de_sas_dpia_list_en.pdf veröffentlicht. Eine Anpassung in Bezug auf die aufgeführten Empfehlungen wurde in der UAG DSFA vorgenommen. Hier steht noch eine erneute Abstimmung in der DSK aus. Ich werde fortwährend auf meiner Web-Präsenz informieren, wenn es hier Änderungen gibt. Verantwortlichen und Auftragsverarbeitern ist zu empfehlen, für Verarbeitungen, die durch eine Konsultation der zuständigen Datenschutzaufsichtsbehörde gemäß Art. 36 DS-GVO genehmigt sind bzw. genehmigt werden sollten, die zum entsprechenden Zeitpunkt aktuelle MUSS-Liste vorzuhalten.

Anwendung und Ausblick

In Hinblick auf die EU-weite Abstimmung ist festzustellen, dass eine Vereinheitlichung nationaler MUSS-Listen zur Durchführung einer DSFA noch eine Weile dauern wird. Inzwischen liegen zusätzlich fünf Einreichungen weiterer EU-Mitgliedstaaten und von Mitzeichnern der DS-GVO wie Norwegen zur Stellungnahme durch den EDSA vor. Diese Einreichungen wurden noch nicht von der Expertengruppe „Technical Subgroup“ entsprechend eines Vorgehens, vergleichbar dem vom September 2018, bewertet. Denn auch hier ist in den Blick gerückt, dass IT-Entwicklungen ein europaweiter Einsatz zu ermöglichen ist.

Von besonderem Interesse scheint mir zu sein, wie sich die Anforderungen in der MUSS-Liste zur Durchführung einer DSFA in der Praxis bewähren. Weitere Einflüsse aus der rechtlichen Praxis werden zu berücksichtigen sein, insbesondere vor dem Hintergrund innewohnender Anforderungen an die technische Umsetzung

– in Verzeichnissen der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO,
– für die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO oder
– beim Einbringen von Zertifizierungen gemäß Art. 42 und Art. 43 DS-GVO.

Die Akzeptanz und die Wirkung der MUSS-Liste wird stark davon abhängen, ob eine europaweite Angleichung die Entwicklung und Nutzung von IT-Systemen in komplexen und komplizierten IT-Landschaften voranbringt, sodass eine DS-GVO-konforme Verarbeitung gewährleistet wird.

4.10.3
Datenschutzfolgenabschätzung nach dem Methodik-Modell der französischen Aufsichtsbehörde

Ab dem 25.05.2018 hat der Verantwortliche gemäß Art. 35 Abs. 1 DS-GVO vorab eine Datenschutzfolgenabschätzung durchzuführen, wenn die bezweckte Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Datenschutzfolgenabschätzung enthält eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und -zwecke, Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, Risikobewertung und Maßnahmen zur Bewältigung der Risiken. Hierfür ist eine strukturierte Dokumentation erforderlich, die dauerhaft zur Verfügung stehen soll. Als Beispiel kann die Software-Plattform der französischen Aufsichtsbehörde dienen.

Die französische Datenschutzaufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat für die Durchführung der Datenschutzfolgenabschätzung (DSFA) (engl. Privacy Impact Assessment, kurz: PIA) gemäß Art. 35 DS-GVO eine Software-Plattform entwickelt und zur Nutzung bereitgestellt (Quelle: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment, letzter Aufruf: 10.12.2018). Ich habe die Software-Plattform in der deutschsprachigen Fassung und in Hinblick auf eine mögliche Anwendbarkeit in kleinen und mittleren Unternehmen (KMU) getestet.

Ablauf des Verfahrens

Die Durchführung der DSFA mit der Software-Plattform der CNIL startet unter der Annahme, dass eine völlig neue Verarbeitung personenbezogener Daten entwickelt wird. Sie basiert auf einem Fragenkatalog, der sich am Verordnungstext der DS-GVO orientiert und sich in vier Teile gliedert: (1) Kontext, (2) grundlegende Prinzipien, (3) Risiken und (4) Bestätigung.

Im Einstieg ist der **Kontext** der Verarbeitungstätigkeit zu beschreiben. Dazu gehört es,

– die Zuständigen,
– zusätzliche, rechtliche Normen, wie Spezialgesetzgebungen, und
– ggf. eingesetzte technische Normen bzw. Standards

zu benennen.

Weiter wird verlangt, die zu verarbeitenden Daten und ihre dazugehörigen Prozesse im Einsatz unter Angabe einer oder mehrerer konkreter IT-Anwendungen zu identifizieren. Es empfiehlt sich daher, entsprechende Verzeichnisse der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO vorab bereitzulegen. Darin müssen bereits die rechtlichen Grundlagen einer Verarbeitung personenbezogener Daten gemäß der Art. 5 bis Art. 7, ggf. Art. 8 oder auch Art. 9 DS-GVO festgehalten sein.

Ferner sind im Verzeichnis der Verarbeitungstätigkeiten Grundzüge im Vorgehen gemäß Art. 24 DS-GVO oder auch Art. 28 DS-GVO sowie die Umsetzung mit technischen und organisatorischen Maßnahmen für einen geplanten gemäß Art. 25 DS-GVO und einen dauerhaften Betrieb gemäß Art. 32 DS-GVO zu dokumentieren.

Schließlich sollte die Risikobetrachtung, für die eine DSFA durchzuführen ist, bereits erfolgt sein. Wenn ein hohes Risiko nicht eingedämmt werden kann, dann ist der Verantwortliche verpflichtet, die zuständige Datenschutzaufsichtsbehörde vor Beginn der Verarbeitung personenbezogener Daten gemäß Art. 36 DS-GVO zu konsultieren; s. a. Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, z. B. unter https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk, letzter Aufruf: 12.12.2018).

Im zweiten Schritt ist unter dem Stichwort der **grundlegenden Prinzipien** für die zukünftige Verarbeitungstätigkeit zu untersuchen, ob die Rechtmäßigkeit und die Verhältnismäßigkeit der Verarbeitung personenbezogener Daten gewahrt wird. Dabei ist der Verarbeitungszweck zu bestimmen und zu prüfen, ob dieser Zweck im Einklang mit der DS-GVO steht. Hierzu sind Anforderungen aus Art. 5 DS-GVO zu betrachten. Dazu sind Fragen zu beantworten, die sich z. B. auf die Berücksichtigung der Datenminimierung, der Speicherdauer oder auf die Richtigkeit der Verarbeitung beziehen. Die Antworten müssen im Kontext der ggf. zu betrachteten Spezialgesetzgebungen und technischen Standards gegeben werden.

Als dritter Schritt werden die **Risiken** der Verarbeitungstätigkeit betrachtet, die in direktem Bezug zu den zu ergreifenden technischen und organisatorischen Maßnahmen stehen. Der Bezug zu begleitenden organisatorischen Maßnahmen wird allerdings nur indirekt hergestellt. Im Zentrum stehen in diesem Teil der DSFA IT-Sicherheitsmaßnahmen wie Verschlüsselung, Anonymisierung, Datentrennung, Zutritts-, Zugangs- und Zugriffskontrolle,

Protokollierung im Sinn der Rückverfolgbarkeit und andere mehr. Auch die Bewertung der zu ergreifenden technischen Maßnahmen folgt aus der Perspektive der IT-Sicherheit.

Die Durchführung einer DSFA schließt im vierten Schritt mit einer sogenannten **Bestätigung** ab. Diese umfasst eine Risikomatrix, die in der Software-Plattform als Risikokartierung bezeichnet ist. Diese Risikokartierung ähnelt einer Risikomatrix, wie sie aus den technischen Normen der ISO/IEC 31000er-Reihe zum Risikomanagement bekannt ist. Die Erstellung einer solchen Risikomatrix ist i. d. R. vom unternehmensinternen Risikomodell abhängig.

Das Risikomodell der CNIL-Methodik einer DSFA

Die Software-Plattform CNIL wendet ein IT-Sicherheits-getriebenes Risikomodell an, mit dem die möglichen Einsatzgebiete und dazugehörigen Anwendungsfälle aus Organisations- oder Unternehmenssicht bewertet werden. Im Zentrum der Betrachtung stehen Risiken, von denen eine Gefahr in Abhängigkeit einer möglichen Eintrittswahrscheinlichkeit ausgehen kann. Die Eintrittswahrscheinlichkeiten dieser Risiken ergeben sich aus einem eigenen organisations- oder unternehmensspezifischen Risikomodell, das i. d. R. ein Bestandteil qualitätssichernder Prozesse zur Herstellung eines Produkts ist. Hier ist also die Schwere eines möglichen Risikos für den Fall bewertet, dass ein fehlerhaftes, folglich funktionseingeschränktes bis funktionsuntüchtiges Produkt zum Einsatz kommt. In einem solchen Risikomodell wird zur Kalkulation für die mögliche Schwere eines Schadens auf mögliche Folgeschäden im Einsatzgebiet bzgl. des Anwendungsfalls eines fehlerhaften, funktionseingeschränkten oder gar funktionsuntüchtigen Produkts Bezug genommen. Die Schwierigkeiten, die aus diesem Ansatz resultieren, ergeben sich aus unterschiedlichen Interpretationen, was als Risiko gilt bzw. ein solches darstellen könnte.

Aus datenschutzrechtlicher Sicht ist die Betrachtung der Risiken auf Fragen der IT-Sicherheit verengt. Tatsächlich wird keine Risikobetrachtung unter Berücksichtigung weiterer datenschutzrechtlicher Anforderungen vorgenommen. Es wird auf einzelne bekannte Risiken Bezug genommen, die mehrheitlich aus dem Bereich der IT-Sicherheit abgeleitet sind. Gemäß Art. 32 DS-GVO sollte eine umfassendere Betrachtung möglicher Risiken in Abhängigkeit ihrer Schwere und ihrer Eintrittswahrscheinlichkeit erfolgen. Die DS-GVO-einhergehenden Neuerungen für den Bereich der Informationstechnik sind noch nicht vollständig in der Anwendung der Software-Plattform der CNIL integriert. Aus Sicht der IT sollten deshalb hier auch z. B. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste betrachtet werden (Art. 32 Abs. 1 lit. a DS-GVO). Die Betrachtung zur Wahrung der

Betroffenenrechte geschieht dabei nur indirekt und findet sich in Teilen in den Prinzipien oder in der Bewertung der Risiken, obwohl der Einsatz dieser Software-Plattform damit beworben wird.

Einsatz durch kleine und mittlere Unternehmen (KMU)

Die Software-Plattform der CNIL kann in unterschiedlicher Weise genutzt oder auch in das eigene Netz einer Organisation oder eines Unternehmens integriert werden. Für die Anwendung in der Praxis wird entscheidend sein, wie eine Organisation oder ein Unternehmen bzgl. der IT-Ausstattung aufgestellt sind.

Für die Installation der Software-Plattform der CNIL ist in kleinen und mittleren Unternehmen eine Separation des Werkzeugs – mindestens durch Virtualisierung – zu empfehlen. Die Speicherung der durchgeführten DSFAs verlangt eine besondere Konfiguration, die z. B. über einen Port 8080 läuft. Unternehmens- oder organisationseigene Sicherungsmaßnahmen für gespeicherte Dokumentationen der jeweiligen DFSA sind vorzunehmen, sodass sie im eigenen Interesse verfügbar bleiben und vertraulich behandelt werden. Des Weiteren ist ein Arbeiten mit konkurrierendem Zugriff durch Personen mit unterschiedlichen Zuständigkeiten wenig empfehlenswert, weil kein Berechtigungskonzept hinterlegt und damit auch kein Rollen- und Rechtekonzept implementiert ist.

Insgesamt ist diese Software-Plattform der CNIL ein erster Ansatz, um sich mit Fragen zur DSFA vertraut zu machen. Ob sie ist für einen dauerhaften Betrieb geeignet ist, wird die Praxis zeigen müssen. Hier konnte z. B. im hausinternen Projekt noch nicht untersucht werden, welche Einflüsse Änderungen über einen längeren Zeitraum zur Folge haben, wenn eine DSFA anzupassen ist bzw. wie stabil sich die Vorhaltung der DFSAs erweisen wird. Eine solche Bewertung eines dauerhaften Einsatzes der Software-Plattform der CNIL ist nicht möglich. Mitentscheidend für die Akzeptanz in KMUs wird sein, inwiefern Weiterentwicklung und Wartung der Software-Plattform der CNIL, z. B. durch Sicherheits-Updates, sichergestellten werden. Hier wird ferner hineinspielen, inwieweit die Kompatibilität gewahrt wird, sodass bereits erstellte DSFAs erneut in der Software-Plattform geöffnet und wieder gespeichert werden können und damit das Vorhalten angepasster DSFAs ermöglicht wird.

4.10.4
Grundlagen und Rahmenbedingungen zu Akkreditierungen und Zertifizierungen gemäß DS-GVO

Mit dem Wirksamwerden der Datenschutz-Grundverordnung sind die Datenschutzaufsichtsbehörden aufgefordert, Zertifizierungen zu fördern. Im Rahmen datenschutzrechtlicher Zertifizierungen sind durch akkreditierte Zertifizierungsstellen datenschutzrechtliche Kriterien gemäß Art. 42 Abs. 5 DS-GVO zu prüfen. In Deutschland dürfen nur durch die Deutsche Akkreditierungsstelle (DAkkS) akkreditierte Zertifizierungsstellen Zertifizierungen nach Art. 42 und Art. 43 DS-GVO i. V. m. § 39 BDSG erteilen. Um datenschutzrechtliche Kriterien durch eine akkreditierte Zertifizierungsstelle unter Anwendung spezifischer Zertifizierungsprogramme prüfen zu lassen, sind ineinandergreifende Prüfverfahren umzusetzen. Dabei handelt es sich um ein bundesweit abgestimmtes Akkreditierungs- und Zertifizierungsverfahren, das DS-GVO-konforme Verarbeitungen personenbezogener Daten gewährleistet.

Akkreditierungen

Mit der Anwendung von Art. 43 DS-GVO ist ein Akkreditierungsverfahren im Einvernehmen zwischen den zuständigen unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder und der DAkkS, die gemäß § 39 BDSG die beliehene Stelle des Bundes zur Durchführung von Akkreditierungen ist, umzusetzen. Gemäß Art. 43 Abs. 1 lit. b DS-GVO ist zudem die Anwendung der technischen Norm EN ISO/IEC 17065 gesetzt, wobei in diesem auch bereits vorgesehen ist, dass weitere Anforderungen der unabhängigen Datenschutzaufsichtsbehörden zu berücksichtigen sind.

Solche weiteren datenschutzrechtlichen Anforderungen, die bei der Akkreditierung von Zertifizierungsstellen durch die DAkkS und die jeweils zuständige Datenschutzaufsichtsbehörde zu prüfen sind, finden sich in „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“, die durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 28.08.2018 beschlossen wurden. Diese Erweiterungen zur DIN EN ISO/IEC 17065 sind unter https://www.datenschutzkonferenz-online.de/media/ah/20180828_ah_DIN17065-Ergaenzungen-full-V10-final_V3_DSK.pdf abrufbar (letzter Aufruf 20.12.2018).

In Bezug auf die tatsächliche Anwendung dieser Erweiterungen ist anzumerken, dass eine verbindliche Stellungnahme des Europäischen Datenschutzausschusses (EDSA) aussteht, auch wenn die Erweiterungen bereits in einem erforderlichen Verfahren nach Art. 64 DS-GVO in deutscher Sprache übermittelt wurden. Hiernach besteht die strittige Anforderung, dass Dokumente, die einem Art. 64-Verfahren unterliegen, nur in englischer Sprache

eingereicht werden können (zur europäischen Zusammenarbeit s. a. 46. Tätigkeitsbericht, Ziff. 4.2).

Auch wenn die vorausgehende Fassung der Veröffentlichung des EDSA zur Akkreditierung „Guidelines 4/2018 on the accreditation of certification bodies under Article of the General Data Protection Regulation (2016/679)“ bei der Erstellung der „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m.: DIN EN ISO/IEC 17065“ berücksichtigt wurde, ist eher davon auszugehen, dass über den Vergleich der Ausgestaltungen dieser datenschutzrechtlichen Anforderungen aus anderen EU-Mitgliedstaaten Anpassungen ebenso in der deutschen Fassung erfolgen werden. Die Veröffentlichung dieser genannten und bereits überarbeiteten Leitlinie findet sich unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en (letzter Aufruf: 20.12.2018). Ein Anhang konkretisiert die EU-weit im EDSA abgestimmten Anforderungen an zu akkreditierende Zertifizierungsstellen; er wurde am 14.12.2018 unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/edpb-guidelines-42018-accreditation-certification-bodies_en vom EDSA veröffentlicht (letzter Aufruf: 20.12.2018).

Gemäß der Hierarchie der technischen Normen ist die Norm EN ISO/IEC 17065 ein Folgenorm der Norm EN ISO/IEC 17065. Im Allgemeinen sind mit der Anwendung der technischen Norm EN ISO/IEC 17067 Inhalte auszugestalten, die die akkreditierten Zertifizierungsstellen im Rahmen eines Zertifizierungsprozesses zu prüfen haben. Sofern ist hier wesentlich, dass die Datenschutzaufsichtsbehörden ihre datenschutzrechtlichen Inhalte darstellen.

Zertifizierungen

Im Akkreditierungsverfahren von Zertifizierungsstellen gemäß Art. 43 DS-GVO ist ein Prüfverfahren hinterlegt, das eine Organisationsprüfung der zu akkreditierenden Zertifizierungsverfahren darstellt. Neben der Prüfung im Rahmen der Akkreditierung sind Prüfverfahren für Zertifizierungen auszugestalten und umzusetzen, die anhand festgelegter datenschutzrechtlicher Kriterien eine Prüfsystematik und -methodik für einen konkreten Zertifizierungsgegenstand ermöglichen.

Erste EU-weite Vorgaben an die Zertifizierungsgegenstände finden sich in einer Leitlinie des EDSA mit dem Titel „Guidelines 1/2018 on certfication and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679“, die bereits am 30.05.2018 veröffentlicht wurde und unter https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-12018-certification-and-identifying_de zu finden ist (letzter Aufruf:

20.12.2018). Eine überarbeitete Fassung dieses Dokuments ist für Anfang 2019 angekündigt. Diese Leitlinie zu Zertifizierungskriterien wird einen Anhang umfassen, der Zertifizierungskriterien gemäß Art. 42 Abs. 5 nochmals konkretisiert.

Beteiligung des HBDI

Seit 2016 ist eine Mitarbeiterin aus dem Bereich der Informationstechnik ständig in dem dafür bundesweit eingerichteten Arbeitskreis „Zertifizierung" unter Federführung des Unabhängigen Landesdatenschutzzentrums Schleswig-Holstein tätig. Diese anspruchsvolle und vielschichtige Tätigkeit erfordert weitere personelle Ressourcen. So sind mittlerweile auch juristische Referate eingebunden.

Drei meiner Mitarbeiterinnen und Mitarbeiter aus den Bereichen der Informationstechnik und des Rechts sind auf der Grundlage entsprechender Ausbildungsgänge und Schulungen zur Durchführung von Akkreditierungen im Einvernehmen mit der DAkkS befähigt.

In Hessen werden im Jahr 2019 mindestens drei Akkreditierungen von Zertifizierungsstellen erwartet, an denen ich mich im Einvernehmen mit der DAkkS beteiligen werde. Ferner werde ich einen verstärkten Fokus auf die notwendigen Prüfkriterien sowie die Prüfsystematik und -methodik legen, sodass in einem Zertifizierungszeitraum dauerhafte Konformität mit der DS-GVO in jeweiligen Zertifizierungsprogrammen gemäß Art. 42 Abs. 1 DS-GVO gewährleistet werden kann. Solche Zertifizierungsprogramme sind von zukünftig akkreditierten Zertifizierungsstellen zu erstellen, weil sie die Basis für datenschutzrechtliche Prüfungen im Rahmen von zu erteilenden Zertifizierungen sind.

Fazit

Aus informationstechnischer Sicht ist eine Beteiligung des HBDI entscheidend, weil Zertifizierungen als Nachweis einer DS-GVO-konformen Verarbeitung in den Art. 30, 32, 35 i. V. m. Art. 36 über ErwGr 90 referenziert werden. Eine Zertifizierung bedeutet immer einen Vorgriff auf eine datenschutzrechtliche Prüfung, die ggf. bei der Erteilung einer Zertifizierung erfolgt. Beim Eingang z. B. einer Beschwerde, die eine datenschutzrechtliche oder informationstechnische Prüfung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO initiieren kann, können von Verantwortlichen Zertifizierungen als Nachweis einer datenschutzkonformen Verarbeitung angeführt werden. Datenschutzrechtliche Anforderungen sowie Prüfkriterien mit Prüfsystematik und -methodik akkreditierter Zertifizierungsstellen müssen zukünftig mit denjenigen konver-

gieren, die bereits heute durch mich umgesetzt sind. Das ist eine wesentliche Voraussetzung, um schließlich erteilte Zertifizierungen ggf. im Rahmen von Sanktionierungen gemäß Art. 83 DS-GVO anerkennen zu können.

4.11
Bußgeldverfahren, Meldungen von Datenpannen

4.11.1
Europäisierung des Bußgeldverfahrens und Kollisionspunkte mit dem nationalen Recht

Der Verordnungsgeber hat es den Mitgliedstaaten gemäß Art. 83 Abs. 8 DS-GVO überantwortet, das Verfahren über die Ahndung von Verstößen gegen die DS-GVO mit angemessenen Verfahrensgarantien zu unterlegen. Aufgrund dieser obligatorischen Öffnungsklausel wurde mit § 41 BDSG eine Brücke zum vorhandenen nationalen Verfahrensrecht im OWiG, Gesetz über das Strafverfahren (StGB) der Strafprozessordnung (StPO) und das Gerichtsverfassungsgesetz (GVG) gebaut. Die Praxis zeigt, dass dies, vorbehaltlich noch ausstehender höchstrichterlicher Rechtsprechung, dem Bundesgesetzgeber europarechtlich nicht kollisionsfrei gelungen ist und es gegebenenfalls nach einer Praxisphase einer Nachbesserung bedarf.

Seit dem 25.05.2018 gilt mit Art. 83 Abs. 4, 5, 6 DS-GVO ein umfangreicher Katalog europaweit anzuwendender Bußgeldtatbestände. Das materielle europäische Datenschutzrecht soll mit nationalen Verfahrensgarantien wirksam, verhältnismäßig und abschreckend durchgesetzt werden. Bei der Umsetzung in das nationale Recht übernimmt § 41 BDSG die Schaltstelle, weil dort die Anwendbarkeit des nationalen Verfahrensrechts und der Umfang der Anwendbarkeit bei der Ahndung von Verstößen gegen die DS-GVO geregelt ist.

Die ersten praktischen Erfahrungen haben gezeigt, dass drei Punkte immer wieder Fragen aufwerfen:

– der sog. „funktionale Unternehmensbegriff“ und die Anwendbarkeit der §§ 9, 30 und 130 OWiG
– die Frage nach einem Bußgeldrahmen oder einer Kappungsgrenze
– die Ahndbarkeit von Art. 33 DS-GVO Meldungen im Bußgeldverfahren

§§ 9, 30 und130 OWiG

Im ersten Entwurf zum Bundesdatenschutzgesetz wurden die §§ 9, 30 und 130 OWiG in der Anwendung noch ausgeschlossen. Die in Kraft getretene Fassung des § 41 Abs. 2 S. 1 BDSG belässt es bei der Anwendbarkeit dieser Normen. Das löst in der Bußgeldpraxis Fragen aus.

§ 41 Abs. 2 Satz 1 und 2 BDSG

Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

Die EU-Ebene geht in der DS-GVO vom funktionalen Unternehmensbegriff aus (s. ErwG 150 Satz 3), stellt auf den Begriff der „wirtschaftlichen Einheit“ ab und erachtet es für eine Bebußung eines Unternehmens oder eines Konzerns für ausreichend, wenn feststeht, dass ein Mitarbeiter oder eine Mitarbeiterin des Unternehmens gegen eine das Unternehmen treffende Pflicht verstoßen hat.

ErwG 150 Satz 3

Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Art. 101 und 102 AEUV verstanden werden.

Mittels der Annahme, dass ein Unternehmen jede Einheit ist, die unabhängig von der Rechtsform und der Art ihrer Finanzierung wirtschaftliche Tätigkeit ausübt (sog. funktionaler Unternehmensbegriff), wird es grundsätzlich möglich, einen ganzen Konzern für den Datenschutzverstoß eines Tochterunternehmens verantwortlich zu machen. Es kommt den Verordnungsgebern der DS-GVO nicht auf die Eigenschaft als Rechtsträger an, sondern nur auf die Ausübung faktischer wirtschaftlicher Funktionen. Der Referenzpunkt „funktionaler Unternehmensbegriff“ dient als Vereinfachungsmechanismus auf der Rechtsfolgenseite. Das europarechtliche Datenschutzbußgeld ist primär auf die Unternehmens-/Verbandsgeldbuße ausgerichtet. Die natürliche Person, die für das Unternehmen tätig war, rückt in den Hintergrund.

Im deutschen Verfahrensrecht der Ordnungswidrigkeiten ist der bewährte § 30 OWiG eine Beteiligungs- und Sanktionsnorm, die die Verhängung von Geldbußen gegenüber Verbänden ermöglicht. Sie ist eine reine Rechtsfolgenregelung. § 30 OWiG liegt das Rechtsträgerprinzip zu Grunde. Das Rechtsträgerprinzip stellt auf bestimmte rechtliche Entitäten und nicht etwa,

wie das europäische Datenschutzrecht, auf die wirtschaftliche Einheit ab. Juristische Person sind demnach alle sozialen Organisationen, denen die Rechtsordnung eine eigene Rechtspersönlichkeit zuerkennt (Göhler /Gürtler OWiG § 30 RdNr. 2), wie z. B. AG, GmbH, die Genossenschaft oder der eingetragene Verein. Als Personenvereinigung ist der juristischen Person die rechtsfähige Personengesellschaft (z. B. OHG, GmbH & Co. KG, KG, GbR) gleichgestellt.

Der Sache nach können Unternehmen nicht selbst handeln. Daher wird ihnen das Verhalten natürlicher Personen gesetzlich zugerechnet. Über die Zurechnungsnormen wird diese Lücke geschlossen. § 30 OWiG knüpft dabei an die Tat einer die Entität repräsentierenden Leitungsperson an. Wer Leitungsperson in diesem Sinne ist, wird in § 30 Abs. 1 Nr. 1 bis 5 OWiG definiert.

Die Aufzählung in § 30 Abs. 1 OWiG wurde zuletzt 2002 um Ziff. 5 erweitert, weil die nationale Gesetzgebung an europäische Anforderungen angepasst werden sollte (BTDrucks. 14/8998, S. 6, 7, 10).

§ 30 Abs. 1 Nr. 5 OWiG

Hat jemand

1. …

…

5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 und 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von Kontrollbefugnissen in leitender Stellung gehört,

eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.

Durch § 30 Abs. 1 Nr. 5 OWiG wurde eine Art Generalklausel eingeführt und der Kreis der Leitungspersonen erheblich ausgedehnt. Maßgeblich ist danach weniger die formelle Rechtsposition, z. B. Geschäftsführer, als das materielle Kriterium des für die Leitung des Unternehmens verantwortlichen Handelnden, also Personen, die zum Kreis der für die Leitung des Betriebs oder Unternehmens verantwortlich handelnden Personen gehören (BT-Drucks. 14/8998, S. 7). Dieser zwar weite Ansatz des nationalen Rechts wird dem EU-Datenschutzrecht dennoch nicht gerecht. Es stellt sich in diesem Kontext die Frage, wie diejenigen Fälle zu handhaben sind, in denen eine Leitungsfunktion nicht nachweisbar ist. Wegen der dadurch möglichen Zuweisungsschwierigkeiten kann eine effektive Sanktionierung von Verstößen

gegen die DS-GVO behindert werden. Es besteht zwar nach § 30 Abs. 4 S. 1 OWiG die Möglichkeit einer „isolierten“ Verbandsgeldbuße. Aber auch für die Verhängung einer „anonymen“ Geldbuße ist festzustellen, dass jedenfalls irgendeine Leitungsperson die Tat begangen hat. Es bedarf eines Handelns als Leitungsperson i. S. d. § 30 Abs. 1 Nr. 1 bis 5 OWiG. Dem kann man unter Umständen mittels einer europarechtskonformen Auslegung von § 30 Abs. 1 Nr. 5 OWiG übergangsweise entgegentreten. Es wäre dennoch wünschenswert, dass der Bundesgesetzgeber prüft, ob und wie man im BDSG, vergleichbar zu den Regelungen im § 81 GWB, spezielle Verfahrensvorschriften zum Ordnungswidrigkeitenrecht verfassen kann. Sofern dieses nicht in Betracht kommt, stellt sich die Frage, ob nicht sogar § 30 Abs. 1 Nr. 5 OWiG im Lichte der europäischen Anforderungen und im Zuge einer Modernisierung unter Berücksichtigung der nationalen verfassungsrechtlichen Anforderungen den aktuellen Anforderungen anzupassen ist.

§ 9 OWiG ist mit § 30 OWiG eng verbunden. Das unterschiedliche Verständnis zwischen europäischer und nationaler Ebene trifft auch § 9 OWiG.

Soweit man das europäische Verständnis zugrunde legt, stellt sich die Frage, ob § 130 OWiG, der ein Tatbestand ist, der einheitlich und abschließend die Verletzung der Aufsichtspflicht regelt, zumindest für den Anwendungsbereich der Tatbestände der DS-GVO obsolet ist. Nach meiner Auffassung kann er im Zusammenhang mit Verstößen gegen die DS-GVO keine Anwendung finden.

Voraussichtlich werden diese offenen Fragen einer gerichtlichen Klärung zugeführt werden.

Bußgeldrahmen oder Kappungsgrenze

Der Bundesgesetzgeber hat mit § 41 Abs. 1 S. 1 BDSG die Anwendbarkeit des § 17 OWiG ausgeschlossen.

§ 41 Absatz 1 Satz 1 BDSG

Für die Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

Damit kann die Aufsicht Bußgelder ab einer Höhe von 0 EUR festsetzen und statt des bisher dem OWiG zugrunde liegenden Bußgeldrahmen die in der EU diskutierte Kappungsgrenze zugrunde legen. Bis dato war ein Bußgeldrahmen vorgesehen mit einem Mindestbußgeld von 5 EUR. Aktuell wird in den Gremien des EDSA, der Taskforce calculate administrative fines,

im Zusammenhang mit der Auslegung der Grundverordnung diskutiert, ob der DS-GVO die Kappungsgrenze oder ein Bußgeldrahmen zugrunde liegt. Europa kennt in der Regel die Kappungsgrenze, das nationale Ordnungswidrigkeitenverfahren kennt den Bußgeldrahmen. Während die Bemessung eines Bußgeldes sich national innerhalb eines Rahmens bewegt, wird bei der Kappungsgrenze zunächst losgelöst von der Kappungsgrenze ein Bußgeld berechnet und im Anschluss dann gekappt. Diese Art der Bußgeldfestsetzung hat jedoch bei den Unternehmen mit sehr hohen Umsätzen zur Folge, dass zwei Unternehmen für ein und dieselbe Tat infolge der Kappung ein und dasselbe Bußgeld für ggf. unterschiedlich schwere Taten zahlen müssten. Das mutet im Ergebnis, wenn der Fall denn überhaupt eintreten sollte, seltsam an, da es dann das gleiche Bußgeld für unterschiedlich schwere Taten gäbe. Allerdings erfordert die Anwendung der Kappungsgrenze, dass der Bußgeldzumessung Leitlinien zugrunde gelegt werden.

Art. 33 DS-GVO und das Bußgeldverfahren

Die Rückmeldungen von Firmen zeigen, dass es dem Bundesgesetzgeber mit der Regelung in § 43 Abs. 4 BDSG gelungen ist, einen unglücklichen Anschein zu erwecken, der zu einer Fehlannahme bei den Betroffenen führt. Die Unternehmen und Einzelpersonen gehen infolge der Regelung davon aus, dass ein Verstoß bzw. eine Datenpanne (data breach), die sie über das „Art. 33er-Portal“ bei der Aufsicht melden, nicht geahndet werden kann.

§ 43 Abs. 4 BDSG

Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Die Unternehmen müssen eine Datenpanne rechtzeitig nach Art. 33 DS-GVO melden, sonst droht nach Art. 83 Abs. 4 DS-GVO ein Bußgeldverfahren. Im Falle der Meldung einer Datenpanne wird seitens der Meldenden aufgrund der Regelung in § 43 Abs. 4 BDSG davon ausgegangen, dass der Sachverhalt für eine Ahndung im Bußgeldverfahren gesperrt sei, außer jener genehmige die Verwendung. Die erste Praxis im Berichtsjahr hat gezeigt, dass vor allem die Wirtschaft davon ausgeht, dass das Melden von Datenpannen von einem Bußgeldverfahren frei mache – und zwar in doppelter Hinsicht.

Richtig ist, dass eine nicht- und nicht rechtzeitige Meldung einer Datenpanne zu einem Bußgeld ^Sm. d. Art. 83 Abs. 4 DS-GVO führt.

Richtig ist aber auch, dass eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach Art. 34 DS-GVO gegen den Meldepflichtigen oder Benachrichtigenden oder sein in § 52 Abs. 1 der StPO bezeichneten Angehörigen nur mit Zustimmung des meldepflichtigen oder Benachrichtigenden verwendet werden kann.

Darüber hinaus ich gehe davon aus, dass, wenn ein Unternehmen eine Datenpanne meldet, dies nicht bedeutet, dass der dort beinhaltete Datenschutzverstoß per se nicht geahndet werden kann. Die Inhalte der Art. 33er-Meldung, die ich im Rahmen des Aufsichtsverfahrens oder eines Bußgeldverfahren selber hätte ermitteln können, kann ich im Bußgeldverfahren ahnden, sofern sie mir bei eigener Prüfung hätten erkennbar werden können. Die in der Rechtsprechung zu § 97 Insolvenzordnung entwickelten Grundsätze sind hier heranzuziehen.

4.11.2
Die ersten Bußgeldverfahren unter dem Regime der DS-GVO

Ungeachtet der Kollisionen, die sich aus der Struktur des deutschen Ordnungswidrigkeitenrechts und dem Sanktionssystem des reformierten europäischen Datenschutzrechts ergeben, bereitet die Anwendung der neuen Tatbestände aus bußgeldrechtlicher Sicht bisher nur wenig Probleme.

Die zu verfolgenden Sachverhalte wurden mir wie auch in den vorangegangenen Berichtszeiträumen von den betroffenen Personen unmittelbar sowie über die Polizei bzw. die Staatsanwaltschaften zur Kenntnis gebracht. Dabei hat die Zahl der zu bearbeitenden Bußgeldfälle im Jahr 2018 erheblich zugenommen. Bereits im August 2018 wurde das Mittel der in den Vorjahren eingeleiteten Ordnungswidrigkeitenverfahren erreicht.

Für Handlungen, die vor dem 25.05.2018 beendet worden sind, gelten aufgrund des in § 4 Abs. 3 des Gesetzes über Ordnungswidrigkeiten (OWiG) statuierten Prinzips der Meistbegünstigung in der Regel weiterhin die Bußgeldvorschriften des § 43 Bundesdatenschutzgesetz (BDSG a. F.) in der Fassung der Bekanntmachung vom 14.03.2003 (BGBl. I. S. 60) sowie der in § 43 Abs. 3 BDSG a. F. normierte Bußgeldrahmen bis 50.000 EUR bzw. 300.000 EUR. Zeitweilig werden daher noch Bußgeldbescheide nach alter Rechtslage erlassen werden.

Hinsichtlich der zu verfolgenden Fälle haben sich nach Änderung der Rechtslage bisher nur geringe Unterschiede ergeben, denn der überwiegende Teil der hier bekannt gewordenen datenschutzrechtlichen Zuwiderhandlungen war bereits nach altem Recht mit Geldbuße bedroht. Die Mehrzahl der in Rede

stehenden Sachverhalte ereignete sich bei der Verarbeitung personenbezogener Daten im Rahmen der Direktwerbung. Damit unterfallen die meisten der derzeit zu verfolgenden Verstöße der Bußgeldvorschrift des Art. 83 Abs. 5 der Datenschutzgrundverordnung (DS-GVO), die im Vergleich zur Regelung des Art. 83 Abs. 4 DS-GVO die Verhängung deutlich höherer Geldbußen vorsieht. In diesem Zusammenhang ist zudem zu beachten, dass Art. 83 Abs. 2 DS-GVO bezüglich der Geldbuße vorgibt, dass diese für Verstöße gegen Art. 83 Abs. 4 bis Art. 83 Abs. 6 DS-GVO in jedem Einzelfall wirksam, verhältnismäßig und zusätzlich auch abschreckend sein soll. Vor diesem Hintergrund sind empfindliche Geldbußen zur effektiven Durchsetzung der Verordnung je nach den Umständen des Falls auch bereits bei vermeintlich „leichteren“ Verstößen möglich.

Unerwünschte Werbe-E-Mails

In einem Verfahren teilte mir die betroffene Person mit, dass sie an einem Gewinnspiel eines in Hessen ansässigen Unternehmens teilgenommen habe. Obwohl die betroffene Person dabei die Bestellung des E-Mail-Newsletters ausgeschlossen habe, habe sie in der Folge von dem Unternehmen eine E-Mail mit werblichem Inhalt erhalten.

Grundsätzlich stellt die Zusendung einer Werbe-E-Mail eine unrechtmäßige Verarbeitung personenbezogener Daten dar, wenn diese nach Ausübung des Widerspruchsrechts gemäß Art. 21 DS-GVO erfolgt oder nicht durch einen Erlaubnistatbestand gedeckt ist. In diesem Kontext begangene Verstöße können nach Art. 83 Abs. 5 lit. a bzw. lit. b DS-GVO mit einer Geldbuße bis 20.000.000 EUR oder im Falle eines Unternehmens bis 4 % des weltweiten Jahresumsatzes belegt werden.

Im konkreten Fall ist das Unternehmen, das den Versand der E-Mail veranlasst hatte, Teil eines Konzerns. Der weltweite Jahresumsatz des Mutterunternehmens liegt im höheren dreistelligen Millionenbereich, sodass vorliegend erstmalig der Anwendungsbereich der prozentualen Obergrenze eröffnet sein könnte. Das Verfahren ist noch nicht abgeschlossen.

Veröffentlichung der Kontaktdaten der oder des Datenschutzbeauftragten

Bisher wurden nur wenige Ordnungswidrigkeitenverfahren wegen Verstößen gegen die neuen Verhaltenspflichten und Verbote der DS-GVO eingeleitet. Einer der ersten zu ahndenden Zuwiderhandlungen gegen eine durch die DS-GVO neu geschaffene Pflicht betraf einen Verstoß gegen Art. 83 Abs. 4 lit. a DS-GVO i. V. m. Art. 37 Abs. 7 DS-GVO.

Im Sommer 2018 wurde mir zur Kenntnis gebracht, dass ein Unternehmen auf seiner Website anstelle der Kontaktdaten der Datenschutzbeauftragten lediglich eine allgemeine Kontaktadresse des Unternehmens aufgeführt hatte. Eine Veröffentlichung der Kontaktdaten der Datenschutzbeauftragten erfolgte auch nicht auf sonstige Weise.

Nach Art. 37 Abs. 7 DS-GVO ist der Verantwortliche oder Auftragsverarbeiter nunmehr verpflichtet, die Kontaktdaten der oder des Datenschutzbeauftragten zu veröffentlichen. Die DS-GVO definiert jedoch nicht, was unter dem Begriff „Veröffentlichung“ konkret zu verstehen ist. Durch die neu eingeführte Pflicht zur Veröffentlichung der Kontaktdaten der oder des Datenschutzbeauftragten sollen die Rechte der betroffenen Personen abgesichert werden. Insbesondere sollen die betroffenen Personen durch die Veröffentlichung jederzeit in die Lage versetzt werden, von ihrem Recht aus Art. 38 DS-GVO Gebrauch zu machen. Hierzu sollen sie sich auf einfachem und direktem Wege in vertraulicher Weise an den Datenschutzbeauftragten wenden können. Denklogisch wird dem Regelungszweck nicht durch eine einmalige oder kurzzeitige Veröffentlichung der Kontaktdaten Genüge getan, sodass dieser nur durch eine permanente Auffindbarkeit der Kontaktdaten erreicht werden kann. Eine Maßnahme der Veröffentlichung, die den Anforderungen des Art. 37 Abs. 7 DS-GVO entspricht, stellt beispielsweise die Angabe der Kontaktdaten der oder des Datenschutzbeauftragten an einer gut auffindbaren Stelle auf der Website (Datenschutzerklärung, vgl. Art. 13 Abs. 1 lit. b DS-GVO) dar. Die dauerhafte Einsehbarkeit der Kontaktdaten ermöglicht es den betroffenen Personen, jederzeit Kontakt zu der oder dem Datenschutzbeauftragten aufzunehmen.

Verstöße gegen Art. 83 Abs. 4 lit. a DS-GVO i. V. m. Art. 37 Abs. 7 DS-GVO können mit einer Geldbuße bis 10.000.000 EUR oder im Falle eines Unternehmens bis 2 % des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist, geahndet werden. Gerade vor dem Hintergrund der erheblichen Bußgeldandrohung sollten Verantwortliche oder Auftragsverarbeiter stets darauf achten, dass betroffenen Personen die Möglichkeit zur Verfügung steht, auf unmittelbarem Wege an die oder den Datenschutzbeauftragten heranzutreten. Hierzu kann eine persönliche E-Mail-Adresse bzw. Funktions-E-Mail-Adresse (z. B. „datenschutz@...“), eine Telefonnummer zur direkten Kontaktaufnahme und/oder eine konkrete postalische Adresse der oder des Datenschutzbeauftragten in geeigneter Weise bereitgestellt werden. Die Angabe des Namens der oder des Datenschutzbeauftragten ist hingegen nicht erforderlich, wobei dessen Nennung zu empfehlen ist (vgl. Artikel 29-Datenschutzgruppe, WP 243 rev.01, 2.6).

4.11.3
Meldung der Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO

Verletzungen des Schutzes personenbezogener Daten sind nach Art. 33 DS-GVO an die Aufsichtsbehörde zu melden, es sei denn, ein Risiko für die Rechte und Freiheiten der Betroffenen kann ausgeschlossen werden.

Die Verletzung des Schutzes personenbezogener Daten (Datenpanne) löst bei Erfüllung der vom Verordnungsgeber in Art. 33 DS-GVO definierten Voraussetzungen eine Pflicht zur Meldung des Vorfalls an die Aufsichtsbehörde aus. Hierbei handelt es sich allerdings nicht um eine neue Regelung. Auch in dem vor der DS-GVO anzuwendenden BDSG a. F. gab es mit dem § 42a BDSG a. F. eine derartige Norm, die sich inhaltlich allerdings deutlich von den Regelungen des Art. 33 DS-GVO abhob.

§ 42a BDSG a. F.

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

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

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

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen

des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Art. 33 DS-GVO

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels.

Feststellung der Pflicht zur Meldung

Beim Vergleich beider Normen werden einige wesentliche Unterschiede erkennbar.

Während nach § 42a BDSG a. F. eine Meldepflicht erst durch eine Datenpanne mit bestimmten Datenarten ausgelöst wurde, verzichtet der Verordnungsgeber auf eine derartige Einschränkung. Auch mussten diese Daten nach der „alten" Norm unrechtmäßig übermittelt oder einem Dritten unrechtmäßig zur Kenntnis gelangt sein. Diese Einschränkung findet sich im Art. 33 DS-GVO nicht.

Das bedeutet, dass seit dem 25.05.2018 jede Verletzung des Schutzes personenbezogener Daten zu einer Meldepflicht nach Art. 33 DS-GVO führen kann. Das könnte beispielsweise auch die unbeabsichtigte Vernichtung von wichtigen und schwer wieder zu beschaffenden personenbezogenen Daten sein, was nach den Regelungen des § 42a BDSG a. F. hingegen keine Meldepflicht ausgelöst hätte.

Dennoch löst nicht jede Datenschutzverletzung automatisch die Pflicht zur Meldung aus. Sowohl der Gesetz- als auch der Verordnungsgeber hat diesbezüglich eine Risikobeurteilung in die jeweiligen Normen mit aufgenommen. Während nach § 42a BDSG a. F. das Drohen einer schwerwiegenden Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen die Meldepflicht auslöste, hat der Verordnungsgeber die Hürde deutlich herabgesetzt. Nunmehr ist nur dann noch von einer Meldung an die Aufsichtsbehörde abzusehen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der natürlichen Person führt. In jedem Einzelfall ist daher eine Prognoseentscheidung zu treffen, die auch entsprechend dokumentiert werden sollte, sodass diese bei Unterbleiben der Meldung und gleichzeitiger Beschwerde durch die betroffene Person durch mich überprüft werden kann.

Zusätzlich umfasst der Anwendungsbereich der DS-GVO im Gegensatz zur früheren Rechtslage nach § 42a BDSG a. F. sowohl nicht-öffentliche als auch öffentliche Stellen.

Die Voraussetzungen des Art. 33 DS-GVO werden daher von einer deutlich höheren Anzahl von Fällen erfüllt, was zu einem starken Anstieg von Meldungen in meiner Behörde geführt hat. So gab es im gesamten Jahr 2017 insgesamt 85 Meldungen nach § 42a BDSG a. F., während für das Jahr 2018 insgesamt 681 Meldungen zu verzeichnen sind. Diese Zahlen setzen sich aus 51 Meldungen nach § 42a BDSG a. F. und 630 Meldungen nach Art. 33 DS-GVO zusammen. Betrachtet man nur den Zeitraum ab dem 25.05.2018, kann von einer jährlichen Fallzahl von etwa 1.000 ausgegangen werden, was einen Anstieg um 1.176 % im Vergleich zum Vorjahr darstellt.

Rechtsfolgen bei Vorliegen der Meldepflicht

Sofern festgestellt worden ist, dass die Voraussetzungen zur Meldepflicht erfüllt sind, hat der Verantwortliche diese nun gegenüber der Aufsichtsbehörde zu melden. Während die Frist nach § 42a BDSG a. F. noch relativ unbestimmt („unverzüglich“) blieb, hat der Verordnungsgeber eine 72-Stunden-Frist eingeführt (Art. 33 Abs. 1 Satz 2 DS-GVO).

Hierbei ist nicht geregelt worden, auf welchem Weg die Meldung zu übermitteln ist. Denkbar sind verschiedene Möglichkeiten, wie der Postweg, per

Fax, per E-Mail (idealerweise verschlüsselt) oder per Meldung über das Meldeportal meiner Homepage, auf der ich ein Formular mit allen für die Meldung erforderlichen Datenfeldern bereitstelle.

Während ein meldepflichtiger Vorfall nach § 42a BDSG a. F. in jedem Fall zusätzlich zur Meldung bei der Aufsichtsbehörde eine Pflicht zur Benachrichtigung der betroffenen Person auslöste, hat der Verordnungsgeber nun differenziert. Eine Benachrichtigungspflicht besteht nur dann, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der natürlichen Person zur Folge hat (Art. 34 DS-GVO). Auch hier ist jeder Einzelfall zu prüfen.

Art. 34 DS-GVO

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,

b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht,

c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

§ 43 Abs.4 BDSG schränkt die Konsequenzen einer Meldung nach Art. 33 DS-GVO für ein Bußgeldverfahren ein.

§ 43 Abs. 4 BDSG

Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Das Unterlassen der Meldung kann ein Bußgeld zur Folge haben. Ebenfalls können Verstöße gegen etwaige Anordnungen seitens der Aufsichtsbehörde, die als Folge nach Art. 33 DS-GVO erlassen worden sind, oder bei der Überprüfung des Vorfalls festgestellte (neue, weitere oder weitergehende) Datenschutzverletzungen entsprechend geahndet werden (siehe hierzu auch Ziff. 4.11.1).

Abschließend kann festgehalten werden, dass die Regelungen der DS-GVO zu einer intensiven Auseinandersetzung der verantwortlichen Stelle mit dem Datenschutzverstoß und deutlich häufiger zu einer Meldung der Datenschutzverletzung an die Aufsichtsbehörde führt.

Abgabe einer Meldung nach Art. 33 DS-GVO

Bei einer Meldung nach Art. 33 Abs. 1 DS-GVO sind die Mindestanforderungen aus Art. 33 Abs. 3 zum Inhalt und Umfang der bereitzustellenden Informationen zu erfüllen. Um Verantwortliche dabei zu unterstützen, steht auf meiner Website unter https://datenschutz.hessen.de/service/meldungen-von-verletzungen-des-schutzes-personenbezogener-daten ein digitales Formular zum Herunterladen zur Verfügung. Aufbau und Inhalt dieses Formulars sind europaweit abgestimmt. Verantwortlichen empfehle ich die Verwendung des Formulars und dessen gewissenhaftes Ausfüllen, um sicherzustellen, dass sie ihre Pflichten nach Art. 33 Abs. 3 DS-GVO erfüllen.

Zur Übermittlung eines ausgefüllten Formulars an mich, und somit zur Abgabe einer Meldung nach Art. 33 Abs. 1 DS-GVO, stehen Verantwortlichen unterschiedliche Übermittlungswege offen. Zusätzlich zur postalischen Übersendung des ausgedruckten Formulars habe ich zwei digitale Übermittlungsalternativen eröffnet. Verantwortliche sollen hierdurch in die Lage versetzt werden, ihrer Verpflichtung zur Einhaltung der 72-Stunden-Frist nach Art. 33 Abs. 1 DS-GVO uneingeschränkt nachzukommen. Eine Meldung ist somit unabhängig von den Öffnungszeiten meiner Behörde jederzeit möglich.

Als erste, digitale Alternative besteht die Möglichkeit der Übermittlung einer Meldung als E-Mail-Anhang. Hierbei ist zu beachten, dass Meldungen nach Art. 33 Abs. 1 DS-GVO häufig sensible Informationen enthalten. Um deren

Schutzbedarf gerecht zu werden, sollten entsprechende E-Mails ausschließlich Ende-zu-Ende-verschlüsselt übermittelt werden. Nähere Informationen zum verschlüsselten E-Mail-Versand können auf meiner Website unter https://datenschutz.hessen.de/service/verschl%C3%BCsselte-kommunikation-mit-dem-HBDI nachgelesen werden.

Im Rahmen der Vorbereitung auf das Wirksamwerden der DS-GVO am 25.05.2018 habe ich eine weitere digitale Möglichkeit zur Abgabe einer Meldung nach Art. 33 Abs. 1 DS-GVO geschaffen. Diese ist über meiner Website unter https://datenschutz.hessen.de/service/meldungen-von-verletzungen-des-schutzes-personenbezogener-daten nutzbar und zeichnet sich durch einfache Bedienbarkeit aus. Insbesondere sind zur Nutzung außer einem E-Mail-Account keine weiteren Voraussetzungen zu erfüllen. Als Grundlage der Übermittlung des ausgefüllten Formulars kann auf der obigen Seite ein sogenannter Upload-Link angefordert werden. Hierbei handelt es sich um einen für die Meldung spezifischen Hyperlink, der an eine vom Verantwortlichen angegebene E-Mail-Adresse versendet wird. Beim Öffnen des Upload-Links in einem Browser wird eine Seite in HessenDrive, einer sicheren Austauschplattform für digitale Dokumente, geöffnet. Hier wird die Möglichkeit zum Hochladen des ausgefüllten Formulars und etwaiger ergänzender Dokumente geboten. Im Rahmen des Hochladens wird durch den Einsatz entsprechender Verschlüsselungen sichergestellt, dass nur die in meiner Behörde zuständigen Mitarbeiter die übermittelten Dokumente abrufen können. Durch den Einsatz von HessenDrive wird dem Schutzbedarf sensibler Informationen Rechnung getragen.

Zusammenfassend stehen Verantwortlichen zur Abgabe von Meldungen nach Art. 33 Abs. 1 DS-GVO mehrere Übermittlungsalternativen zur Verfügung. Durch die Bereitstellung dieser Alternativen sollen Verantwortliche bei der Abgabe von Meldungen, und insbesondere bei der Einhaltung der 72-Stunden-Frist, bestmöglich unterstützt werden.

4.11.4
Erfahrungsbericht und Statistik zu den Meldungen gemäß Art. 33 DS-GVO im Gesundheitsbereich

Vor dem Wirksamwerden der DS-GVO war in Hessen nur eine Meldepflicht für den privaten Bereich vorgesehen. Mit dem Art. 33 DS-GVO ist nach dem 25.05.2018 nunmehr auch eine Meldepflicht von Datenschutzvorfällen für den öffentlichen Bereich vorgesehen. Die ersten Auswirkungen dieser neuen Regelungen auf den Gesundheitsbereich sollen im Folgenden dargestellt werden.

Sachstand in den ersten drei Monaten nach Inkrafttreten der DS-GVO

In den ersten drei Monaten nach dem 25.05.2018 sind insgesamt 42 Meldungen nach Art. 33 DS-GVO betreffend den Gesundheitsbereich beim HBDI eingegangen. Auf das Jahr hochgerechnet wird damit künftig von bis zu 160 Meldungen im Jahr ausgegangen. Zum Vergleich sei hier darauf hingewiesen, dass für das gesamte Jahr 2017 lediglich 85 Meldungen gemäß § 42a BDSG für alle Bereiche im Haus angefallen sind.

Die 42 Meldungen aus dem Gesundheitsbereich setzen sich schwerpunktmäßig wie folgt zusammen:

– 14 Fälle wegen fehlerhaften Postversands
– 9 Fälle wegen Einbruchs und Diebstahls
– 5 Fälle wegen Hackerangriffen
– 4 Fälle wegen Verlusts von USB-Sticks und Datenträgern
– 3 Fälle wegen unberechtigter Zugriffe auf Datenbanken
– 1 Fälle wegen fehlerhafter Einrichtung von Zugriffsrechten
– 6 Fälle wegen sonstiger Ereignisse

Bewertung der Statistik

Der fehlerhafte Postversand stellt aktuell den häufigsten Meldefall nach Art. 33 DS-GVO dar. Dies ist insbesondere im Bereich Gesundheit wenig überraschend, da der Informationsaustausch zwischen den vielen beteiligten Stellen und Verantwortlichen aufgrund einer gesetzlichen Grundlage oder der Einwilligung der Betroffenen tagtäglich in großer Zahl praktiziert wird. Ich gehe davon aus, dass hier künftig mit geringeren Meldezahlen zu rechnen ist, da sich Erfahrungswerte bilden werden, wann der Fehlversand den Charakter eines meldepflichtigen Ereignisses hat. Zudem denke ich, dass es hier künftig in Ergänzung zu dem Kurzpapier der DSK ein „best practice Paper“ geben wird.

Bei den Meldungen aufgrund von Einbrüchen und Diebstählen sehe ich eher eine wachsende Zahl an Fällen. Gleiches gilt für den Bereich der Hackerangriffe, für die sich Unternehmen und öffentliche Stellen im Gesundheitsbereich verstärkt wappnen sollten (siehe hierzu auch die Kleine Anfrage aus dem Hessischen Landtag vom 12.04.2018 betreffend IT-Sicherheit in Krankenhäusern und die hierzu ergangenen Rückmeldungen, LTDrucks. 19/6275).

Dem Verlust von USB-Sticks und Datenträgern kann künftig dadurch begegnet werden, dass die darauf gespeicherten Daten dem gängigen Standard entsprechend verschlüsselt werden. Aufgrund ihrer Größe neigen insbesondere USB-Sticks schnell dazu, verloren zu gehen.

Ein wichtiges Thema sind für mich die unberechtigten Zugriffe auf Datenbanken. So ist es in einem Fall der betroffenen Klinik nicht aufgefallen, dass mehrere Zugriffskonten von ehemaligen Mitarbeitern nicht ordnungsgemäß gesperrt wurden. Dies erinnert an einen bekannt gewordenen Fall aus Portugal, demzufolge in einem Krankenhaus 985 aktive Benutzer im Krankenhausinformationssystem mit dem Profil „Arzt“ registriert waren, obwohl lediglich 296 Ärzte in dem Krankenhaus arbeiteten (siehe https://www.publico.pt/2018/10/22sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479).

Ausblick und Hinweise für die Zukunft

Für die Zukunft scheint es mir noch einmal wichtig, daran zu erinnern, dass auch der Verlust und die Zerstörung von Patientenakten gemäß Art. 5 Abs. 1 lit. f DS-GVO meldepflichtig ist. So gab es in der Vergangenheit mehr als zwei Arztpraxen in Hessen, bei denen Wasserschäden zur Zerstörung und Unlesbarkeit eines Teils der Patientenakten geführt haben (siehe hierzu auch den Beitrag unter Ziff. 4.6.3 in diesem Tätigkeitsbericht).

Für die weitere Bearbeitung der Vorgänge ist es im Übrigen hilfreich, wenn die Freitextfelder im Meldeformular für detaillierte Beschreibungen der Vorgänge genutzt werden. Hierbei sind unbestimmte Begriffe wie „ungeschützter PC“ zu vermeiden. Zudem sollte der Fehlversand möglichst genau dargestellt und beschrieben werden.

Eine allgemeine Darstellung zur Meldung von Datenschutzverletzungen, die auch den nicht-öffentlichen Bereich betrifft, habe ich unter Ziff. 4.11.3 dargestellt.

4.12
Arbeitsstatistik ab 25.05.2018

Mit Geltung der DS-GVO haben sich auch die Anforderungen zur Darstellung der Arbeitsstatistik geändert.

Art. 59 DS-GVO bestimmt nunmehr, dass der Jahresbericht einer Aufsichtsbehörde eine Liste der Arten der gemeldeten Verstöße und der Arten der getroffenen Maßnahmen nach Art. 58 Abs. 2 DS-GVO enthalten kann. Der Bericht ist nicht nur dem Hessischen Landtag, der Regierung und der Öffentlichkeit vorzulegen, sondern auch der EU-Kommission und dem Europäischen Datenschutzausschuss zugänglich zu machen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben

beschlossen, der Berichtspflicht mit einem jeweils gesonderten und für alle Aufsichtsbehörden einheitlich gestalteten Kapitel „Zahlen und Fakten“ in ihren Tätigkeitsberichten nachzukommen. Damit soll Transparenz und Vergleichbarkeit innerhalb der DSK und für die Öffentlichkeit ermöglicht werden. Da mit diesen Werten nicht alle Tätigkeiten der einzelnen Aufsichtsbehörden abgedeckt werden, können in einem weiteren Kapitel ergänzende Erläuterungen und Darstellungen erfolgen.

4.12.1
Zahlen und Fakten

Zahlen und Fakten	**Fallzahlen 25.05.2018 bis 31.12.2018**
a) Beschwerden	
Anzahl von Beschwerden, die im Berichtszeitraum nach DS-GVO eingegangen sind. Als Beschwerden werden bei Eingang solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, auf die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische Beschwerden werden nur dann gezählt, wenn sie verschriftlicht werden (z. B. durch Vermerk).	**2.278**
b) Beratungen	
Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	**2.185**
c) Meldungen von Datenschutzverletzungen	
Anzahl schriftlicher Meldungen	**630**
d) Abhilfemaßnahmen	
Anzahl der getroffenen Maßnahmen, die (1) nach Art. 58 Abs. 2a (Warnungen) (2) nach Art. 58 Abs. 2b (Verwarnungen) (3) nach Art. 58 Abs. 2c bis g und j (Anweisungen und Anordnungen) (4) nach Art. 58 Abs. 2i (Geldbußen) (5) nach Art. 58 Abs. 2h (Widerruf von Zertifizierungen) im Berichtszeitraum getroffen wurden.	 (1) **0** (2) **2** (3) **2** (4) **0** (5) **0**
e) Europäische Verfahren	
(1) Anzahl der Verfahren mit Betroffenheit (Art. 56) (2) Anzahl der Verfahren mit Federführung (Art. 56) (3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	(1) **120*** (2) **3*** (3) **83*** *Geringfügige Abweichungen möglich
f) Förmliche Begleitung bei Rechtsetzungsvorhaben	
Hier werden pauschaliert als Gesamtzahl die von Parlament/Regierung angeforderten und durchgeführten Beratungen genannt. Dies umfasst auch die Teilnahme in öffentlichen Ausschüssen und Stellungnahmen gegenüber Gerichten.	**14**

Im zweiten Halbjahr 2018 wurden darüber hinaus zwei Ordnungswidrigkeitenverfahren wegen Verstößen gegen die DS-GVO abgeschlossen. Nach den ersten Ermittlungshandlungen wurde deutlich, dass der sachliche Anwendungsbereich der Verordnung nicht eröffnet war. Die Verfahren mussten daher eingestellt werden.

4.12.2
Ergänzende Erläuterungen zu Zahlen und Fakten

Die Werte der Tabelle geben zwar einen Überblick über die Tätigkeiten meiner Mitarbeiterinnen und Mitarbeitern im Bereich der Beschwerden und Beratungen, allerdings kommen Spezifika, die täglichen An- und Herausforderungen sowie eine themenspezifische Bewertung darin nicht zum Ausdruck.

Mit Geltung der DS-GVO und der folgenden vielfältigen – in der Sache nicht immer zutreffenden – Berichterstattung in den Medien änderte sich die Arbeitssituation meiner Behörde ab 25.05.2018 schlagartig. Von einem Tag zum nächsten setzte ein Anfrageansturm per Telefon, E-Mail und Briefpost ein, der mit denselben personellen Ressourcen wie zuvor zu bewältigen war.

Insbesondere die fernmündlichen Anfragen zur DS-GVO brachten die Kapazitäten meiner Mitarbeiterinnen und Mitarbeiter und selbst die der Telefonanlage an die Grenzen der Belastbarkeit. Die telefonischen Beratungen fanden keinen Niederschlag in Akten, nahmen aber erhebliche Zeit und Ressourcen in Anspruch.

Eine Stichprobenzählung für den Monat Juni 2018 ergab 1.703 telefonische Beratungen, die länger als 10 Minuten dauerten (zum Vergleich: noch im April 2018 waren es 484 telefonische Beratungen). Hunderte von ungezählten Anrufen liefen zudem bei den Kolleginnen meiner Geschäftsstelle auf, um dort entweder kurze Auskünfte zu erfragen oder sich darüber zu beschweren, dass die/der zuständige Sachbearbeiter/-in telefonisch nicht zu erreichen bzw. der Telefonanschluss ständig besetzt sei.

Die schriftliche Bearbeitung der Eingaben und Anfragen kam daher nur sehr schleppend voran, was wiederum zu Beschwerden wegen langer Wartezeiten führte. Mit einer internen Umorganisation, weiteren studentischen Aushilfen und der Neuregelung der Telefonzeiten konnte die Funktionsfähigkeit meiner Behörde wieder hinreichend geordnet werden.

Die Monate Mai bis August waren die telefonstärksten Monate des Jahres 2018. Ab September 2018 beruhigte sich die Lage etwas. Bis Ende des Jahres haben sich die mündlichen Auskünfte und Beratungen auf ca. 506 Telefonate im Monat eingependelt. In gleichem Maße, in dem die telefonischen Beratungsanfragen zurückgingen, erhöhten sich die eingereichten schriftlichen

Beschwerden und Eingaben durch Betroffene sowie die Meldungen von Datenschutzverletzungen von Verantwortlichen (zu Letzterem s. a. Ziff. 4.11.3). Es ist deutlich geworden, dass Bürgerinnen und Bürger ihre Rechte auf Auskunft, Berichtigung und Löschung verstärkt einfordern bzw. wünschen, dass bestimmte Sachverhalte einer Überprüfung durch die Aufsichtsbehörde unterzogen werden. So haben sich besonders die Beschwerden im Bereich Auskunfteien und im Gesundheitsbereich im Vergleich zum Vorjahr vervielfacht. Dagegen blieb die befürchtete Abmahnwelle bisher aus.

In über 100 Vorträgen, Schulungen und Workshops bei Vereinen, Wirtschaftsverbänden, sonstigen Vereinigungen, öffentlichen Stellen, dem Hessischen Verwaltungsschulverband (HVSV) und der Zentralen Fortbildung Hessen (ZF) haben meine Mitarbeiterinnen und Mitarbeiter die drängendsten Fragen beantwortet. Im neu gegründeten Arbeitskreis der Datenschutzbeauftragten der obersten Landesbehörden bin ich ebenfalls vertreten.

Viele von mir initiierte Datenschutzprüfungen wurden wegen Zeitmangels zurückgestellt. Es fanden trotzdem noch 15 Prüfungen statt (Vorortprüfungen im Videobereich nicht mitgerechnet), die nicht aufzuschieben waren.

Auch wurden weiterhin sechs Rechtsreferendare und zwei Praktikanten in ihren jeweiligen Stationen ausgebildet.

5. Bilanz

5.1
Digitalisierungsprojekt Schultagebuch für Kinder beruflich Reisender schreitet voran

Im 46. Tätigkeitsbericht habe ich über das Digitalisierungsprojekt DigLu (Digitales Lernen unterwegs) berichtet (Ziff. 9.2). Dabei geht es um die Schaffung einer Lern- und Kommunikationsplattform, um Kindern beruflich Reisender das Lernen zu erleichtern. Wesentlicher Bestandteil dabei ist die Einrichtung eines elektronischen Schultagebuchs. Das Projekt hat im Berichtsjahr einige wesentliche datenschutzrechtliche Hürden genommen.

5.1.1
Die rechtliche Grundstruktur des Projekts ist geschaffen

Die Aufsichtsbehörden der an dem geplanten Pilotprojekt beteiligten Länder Nordrhein-Westfalen, Baden-Württemberg, Niedersachsen, Sachsen, Thüringen und Hessen haben zusammen mit der DigLu-Arbeitsgruppe der Kultusministerkonferenz (KMK) ein Konzept verabschiedet, dem nach dem Testlauf auch die anderen Länder beitreten sollen.

Insbesondere wurde in dem Konzept geklärt, wie das Projekt hinsichtlich Zuständigkeit und Verantwortlichkeit für die Datenverarbeitung gestaltet ist.

So sollen die sechs Pilotländer einen Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO mit dem Dienstleister Jordy Media schließen. Zudem soll im Wege einer Verwaltungsvereinbarung das Land Nordrhein-Westfalen die Systemführung für die Länder übernehmen. Vorgeschaltet ist dem eine Arbeitsgruppe, die die Bedarfe hinsichtlich möglicher Systemerweiterungen und des Supports feststellt und formuliert. Nordrhein-Westfalen übernimmt dann den Kontakt zum Auftragsverarbeiter, erteilt Aufträge und stellt die gegenseitige Kommunikation sicher. Der Auftragsverarbeiter (Jordy Media mit der Software DigLu) bedient sich hinsichtlich der technischen Dienstleistung als Unterauftragsverarbeiter des Netzes der Einrichtung „Baden-Württembergs extended LAN“ (BelWü). Diese betreibt das Netz der wissenschaftlichen Einrichtungen in Baden-Württemberg nebst Rechenzentrumsdienstleistung und steht auch anderen Interessenten für Dienstleistungen zur Verfügung.

5.1.2
Bei Software und Einzelfragen der Verarbeitung personenbezogener Daten besteht noch Klärungsbedarf

Hinsichtlich der Software sind die Funktionalitäten und das Datensicherheitskonzept noch nicht abschließend abgestimmt. Auch hinsichtlich der Einwilligungserklärungen sowie der Informationen i. S. v. Art. 14 DS-GVO gibt es weiteren Klärungs- und Abstimmungsbedarf. Deshalb sind sowohl meine Mitarbeiterinnen und Mitarbeiter als auch die Vertreterinnen und Vertreter anderer Aufsichtsbehörden regelmäßig an den Arbeitstreffen der Arbeitsgruppe DigLu beteiligt, um die datenschutzrechtlichen Rahmenbedingungen der Anwendung sowie deren konkrete Ausgestaltung (z. B. Protokollierung, Rollen- und Berechtigungskonzept, Organisationsstruktur) mitzugestalten. Dabei hat sich ergeben, dass über die klassische Funktion des Klassenbuchs hinaus der Bedarf besteht, die Plattform auch für das Lernen und die Kommunikation zu nutzen. Eine Erweiterung der Funktionalitäten ist grundsätzlich möglich und im Rahmen der Digitalisierungsstrategie der KMK folgerichtig. Allerdings bedarf es hierzu klarer Vorgaben und Regelungen, um dieses bundesweit beispiellose Projekt einer länderübergreifenden Zusammenarbeit im Sinne der betroffenen Kinder zum Erfolg zu führen.

5.1.3
Ausblick

Im Schuljahr 2019/2020 soll das Pilotprojekt starten. Die Anzahl der Kinder soll in einem überschaubaren Rahmen auf zunächst maximal 300 Schülerinnen und Schüler begrenzt werden. Nach der Pilotphase soll eine inhaltliche und technische Evaluierung des Projektes erforderliche Korrekturbedarfe aufzeigen und ggf. eine Optimierung der Software bzw. der Organisationsstruktur erfolgen. In der Endstufe sollen Stamm- und Stützpunktschulen aller 16 Bundesländer mit der Plattform arbeiten und den Kindern eine zeitgemäße Teilhabe an den schulischen Angeboten ermöglichen.

5.2
Datenschutzkonformer Einsatz von Microsoft Office 365 an Schulen (46. Tätigkeitsbericht, Ziff. 9.3)

Mit der Ankündigung der Firma Microsoft, für die Microsoft Cloud Deutschland mit dem Treuhändermodell keine Neukundenverträge mehr zu schließen, stehen Schulen in Hessen erneut vor der Frage, inwieweit der Einsatz der Produkte Microsoft Office 365 bzw. Azure im Kontext der europäischen

Cloudangebote des Konzerns datenschutzrechtlich und hinsichtlich der technischen Ausgestaltung datenschutzkonform umgesetzt werden kann.

Die Änderung des Geschäftsmodells durch Microsoft

Am 31.08.2018 veröffentlichte Microsoft die Ankündigung, keine Neuverträge mehr auf Basis der Microsoft Cloud Deutschland zu schließen. Neukunden können ab 2019/2020 auch auf ein Cloudangebot in Rechenzentren in Deutschland zugreifen, das aber in den weltweiten Standard des Konzerns eingebunden sein wird. Damit wird das Treuhändermodell mit seinen besonderen Gestaltungsmerkmalen den Bestandskunden maximal bis zum zugesicherten Vertragsende zur Verfügung stehen, sofern Kunden nicht vorher schon auf ein Migrationsangebot von Microsoft eingehen. Eine Reihe von Schulen und Schulträgern hatten sich im abgelaufenen Jahr vor dem Hintergrund der deutlich höheren Kosten nicht entschließen können, eine Realisierung mit der Microsoft Cloud Deutschland zu gestalten.

Der AK Verwaltungsmodernisierung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich, nachdem das Treuhändermodell nicht mehr zur Verfügung steht, dazu entschieden, das verbleibende Angebot jetzt unter den rechtlichen Vorgaben und Erwägungen der DS-GVO erneut zu prüfen. Um der Komplexität der Fragestellungen gerecht zu werden, wurde ein eigener Unterarbeitskreis berufen, der unter weitgehender Zurückstellung der technischen Fragen zunächst prüfen wird, inwieweit die Standardverträge geeignet sind, die Anforderungen der Grundverordnung an eine Auftragsverarbeitung zu erfüllen.

Aktuelle Veröffentlichungen zu Office 365 und Windows10

Zum Ende des Jahres wurde durch Veröffentlichungen staatlicher Stellen der Niederlande und Deutschlands publik, dass insbesondere die Übermittlungen von Telemetriedaten an Microsoft selbst für Kunden der Enterprise-Lizenzen ein kaum beherrschbares Problem bei der Nutzung von Office 365 und Windows10 im Umfeld der Cloud darstellen. Diese Problematik habe ich schon in meinem 44. Tätigkeitsbericht (Ziff. 5.1) aufgezeigt.

Für die Schulen und Schulträger stellen sich damit zusätzliche Fragen, mit welchen Maßnahmen die unzulässigen Übermittlungen personenbezogener Daten an Microsoft ausgeschlossen werden können. Verschiedene Lösungsansätze werden dazu gegenwärtig untersucht. Meine Dienststelle befasst sich derzeit erneut mit der Thematik auf der schulischen Ebene und sucht nach sinnvollen und umsetzbaren Alternativen.

5.3
Umgang mit Patientenakten nach Schließung eines Krankenhauses – Die Neuregelung des § 12 Abs. 5 HKHG

In den vergangenen Tätigkeitsberichten wurde wiederholt darüber berichtet, dass derzeit in Hessen keine Regelung betreffend den Umgang mit Patientenakten nach der geplanten oder ungeplanten Schließung eines Krankenhauses existiert. Mittlerweile hat mir das Hessische Ministerium für Soziales und Integration (HSM) einen Entwurf einer entsprechenden Regelung für das zu novellierende Hessische Krankenhausgesetz (HKHG) vorgestellt.

Hintergrund

In der Vergangenheit hatten sowohl geplante als auch ungeplante Schließungen von Krankenhäusern offengelegt, dass der Umgang mit den dazugehörigen Patientenakten nicht hinreichend geregelt war. Insbesondere war es aus meiner Sicht wichtig, dass sowohl die gesicherte Aufbewahrung der Akten in diesen Fällen gewährleistet ist, als auch, dass die ehemaligen Patienten nach wie vor ohne größeren Zeitverlust Einsicht in ihre Patientenakte nehmen können und hierfür auch ein konkreter Ansprechpartner benannt ist.

Mit dem neuen § 12 Abs. 5 HKHG soll dem nun Rechnung getragen werden.

> *§ 12 Abs. 5 HKHG*
>
> *Der Krankenhausträger ist verpflichtet, bei der Schließung eines Krankenhauses oder einer Betriebsstätte eines Krankenhauses dafür zu sorgen, dass die Krankenakten nach den Vorschriften über die Schweigepflicht und den Datenschutz verwahrt werden und nur Berechtigten zugänglich sind.*

Die hier wiedergegebene Fassung stammt vom April 2018. In der Begründung heißt es:

„Die ordnungsgemäße Sicherung und Aufbewahrung von Patientenakten nach Schließung von Krankenhäusern bzw. nach der Schließung von Betriebsstätten eines Krankenhauses ist in den vergangenen Jahren immer wieder diskutiert worden. Die Gesundheitsministerkonferenz (GMK) hat dieses Thema ebenfalls erörtert und Handlungsbedarf bei dem Umgang mit Patientenakten geschlossener Einrichtungen, wie z. B. Krankenhäusern und Reha-Einrichtungen festgestellt. Auch der Hessische Datenschutzbeauftragte hat zuletzt in seinem 45. Tätigkeitsbericht diesen Handlungsbedarf bestätigt. Die Neuregelung des § 12 Abs. 5 HKHG greift den Handlungsbedarf auf und verpflichtet die Krankenhäuser bzw. deren Rechtsnachfolger, bei Schließung eines Krankenhauses oder einer Betriebsstätte eines Krankenhauses dafür

zu sorgen, dass das Recht der Patientinnen und Patienten auf Akteneinsichtnahme gemäß § 630g BGB gesichert ist“.

Rechtliche Bewertung

Zu dem Entwurf habe ich gegenüber dem HSM die folgenden Anmerkungen gemacht:

In den Gesprächen im Jahr 2017 mit dem HSM wurde besprochen, dass die betroffenen Krankenhäuser im Rahmen der Schließung verpflichtend ein Konzept zu erstellen und vorzulegen haben, aus dem hervorgeht, dass und insbesondere wie die Aktenaufbewahrung und die Akteneinsicht sichergestellt wird. Das Konzept könnte sowohl dem HSM als auch dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit verpflichtend vorzulegen sein. Letztlich ist die Beschreibung „bei der Schließung eines Krankenhauses“ relativ unbestimmt, sodass eine genauere Definition erfolgen sollte. Aus meiner Sicht ist es daher erforderlich, schon im Vorfeld, unabhängig von einer drohenden Schließung, ein Verfahren zur Vorgehensweise im Falle einer Schließung (i. S. v. technisch-organisatorischen Maßnahmen) festzulegen.

§ 18 des Berliner Krankenhausgesetzes ordnet auch eine rechtzeitige Informationspflicht gegenüber der Fachaufsicht an, wenn die Schließung eines Krankenhauses absehbar wird (insbesondere im Falle des Antrages auf Eröffnung eines Insolvenzverfahrens). Auch dies sollte m. E. in die Regelung übernommen werden.

Anzudenken wäre auch, ob für den Fall der Insolvenz des Krankenhausträgers selbst nicht noch eine Auffanglösung geschaffen werden kann. Unabhängig davon scheint eine Ergänzung angezeigt, wie sie § 39 Abs. 6 des Landeskrankenhausgesetzes Mecklenburg-Vorpommern (LKHG M-V) vorsieht, da der Krankenhausträger selbst die Akten u. U. nicht in Verwahrung nehmen kann:

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

Inwieweit die von mir gemachten Angaben in den Entwurf aufgenommen wurden, ist mir nicht bekannt.

Zweiter Teil
Erster Bericht zur Informationsfreiheit

1. Einleitung

1.1
Ausdrückliche verfassungsrechtliche Vorgaben

Unter Informationsfreiheit verstand man ursprünglich nur das in Art. 5 Abs. 1 Satz 1GG normierte Grundrecht, sich aus **allgemein zugänglichen Quellen** ungehindert zu informieren. Die Vorschrift knüpft an ältere Landesverfassungen an, die wie Art. 13 HV nach dem Zweiten Weltkrieg vergleichbare Regelungen als Reaktion auf die Informationsunterdrückung im Nationalsozialismus enthielten. Das Grundrecht in Art. 5 Abs. 1 Satz 1 GG ist als reines Abwehrrecht konzipiert und vermittelt keine Informationsansprüche. Über die Zugänglichkeit und die Art der Zugangseröffnung entscheidet, wer nach der Rechtsordnung über ein entsprechendes Zugangsrecht verfügt (BVerfGE 103, 44, 60). Fehlt es an dieser Bestimmung, ist die Informationsbeschaffung nicht vom Grundrecht der Informationsfreiheit geschützt (BVerfGE 66, 116, 137; BGH, NJW 2019, 757, 762). Diese Restriktion besteht nach der Rechtsprechung des Bundesverfassungsgerichts, obwohl das Gericht die verfassungsrechtliche Bedeutung einer informierten Öffentlichkeit in verschiedenen Zusammenhängen nachdrücklich betonte. So führte es aus, nur „umfassende Informationen, für die durch ausreichende Informationsquellen Sorge getragen wird, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft“ (BVerfGE 27, 71). Allerdings umfasse das Grundrecht der Informationsfreiheit ein gegen den Staat gerichtetes Recht auf Zugang in Fällen, in denen eine im staatlichen Verantwortungsbereich liegende Informationsquelle auf Grund rechtlicher Vorgaben zur öffentlichen Zugänglichkeit bestimmt sei, der Staat den Zugang aber verweigere (BVerfGE 103, 41, 60). Das verschafft dem Grundrecht aus Art. 5 Abs. 1 Satz 1 GG jedoch keine Leistungsdimension, auf die etwa Ansprüche auf Auskünfte oder Akteneinsicht gestützt werden könnten. Solche Ansprüche können sich jedoch aus anderen verfassungskräftigen oder einfachgesetzlichen Rechtsgrundlagen ergeben. Derartige Informationsansprüche schließt Art. 5 Abs. 1 Satz 1 GG nicht aus.

1.2
Informationsfreiheitsgesetze

Weitere Informationsansprüche ergeben sich aus den dem Öffentlichkeitsprinzip verpflichteten Informationsfreiheitsgesetzen, die häufig (vgl. Kloepfer, Informationsrecht, 2002, S. 403) auf die schwedische Druckfreiheitsverordnung (Tryckfrihetsförordningen – TF) vom 02.12.1766 zurückgeführt werden, die 1949 unter der gleichen Bezeichnung durch das mit Verfassungsrang ausge-

stattete schwedische Pressefreiheitsgesetz (SFS 1949, 105) ersetzt worden ist. Diese Regelungen betrafen zunächst nur spezielle medienrechtliche Auskunftsansprüche. Zudem wurden Ausnahmen zum Schutz der persönlichen und finanziellen Verhältnisse des Einzelnen zugelassen (Kap. 2 § 2 Nr. 7 TF). Voraussetzungslose allgemeine Informationsansprüche gewährte erst in den USA auf nationaler Ebene der Freedom of Information Act (FOIA), der am 05.07.1967 Geltung erlangte und seitdem mehrfach mit wechselnder Tendenz geändert wurde. Das Gesetz enthält neun Ausnahmen (exemtions), darunter eine Ausnahme zugunsten des Datenschutzes (privacy); hinzu kommt als faktische zehnte Ausnahme die sog. Glomar Response (Ellington, in Marlin/Scott Brady/Kumar, Secrecy, Law and Society, 2015, S. 160). Auf der Website zum FOIA (National.FOIAPortal@usdoj.gov.9) wird in Anlehnung an die Rechtsprechung des Supreme Court die Aufgabe des Gesetzes als demokratische Grundfunktion charakterisiert: „Die grundlegende Funktion des Freedom of Information Act besteht darin, für informierte Bürger zu sorgen, die für das Funktionieren einer demokratischen Gesellschaft lebensnotwendig sind“ („the basic function of the Freedom of Information Act is to ensure informed citizens, vital to the functioning of a democratic society“). Der Supreme Court ging noch weiter: „Die grundlegende Funktion des FOIA sei es, für eine informierte Bürgerschaft zu sorgen, deren Funktionieren benötigt werde, um ein Gegengewicht gegen die Korruption zu schaffen und die Verantwortlichkeit der Regierung gegenüber den Regierten zu gewährleisten“ (NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 [1978]). In Deutschland sah erstmals das brandenburgische Akteneinsichts- und Informationszugangsgesetz (AIG) vom 10.03.1998 (GVBl. I S. 46) voraussetzungslose Auskunftsansprüche vor. Zutreffend wurde das Gesetz nicht als Informationsfreiheitsgesetz bezeichnet. Zweck des Gesetzes war nicht primär der Anspruch auf Informationen, sondern die **Kontrolle der Verwaltung, die durch transparentes Verwaltungshandeln** ermöglicht werden sollte. Die in den späten 1990er Jahren geführte Diskussion über die Notwendigkeit von Informationsfreiheitsgesetzen betraf denn auch weniger die Frage, ob ein allgemeiner Zugang zu öffentlichen Dokumenten als subjektives Recht gewährt werde könne, als die Auswirkungen des Öffentlichkeits- und Transparenzprinzips auf die Qualität des Verwaltungshandelns. Die ambivalente Zielsetzung findet sich mit unterschiedlicher Schwerpunktbildung in allen Informationsfreiheits- und Transparenzgesetzen, die nach 1998 ergingen, nämlich: Bund: Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Bundesinformationsfreiheitsgesetz – IFG) vom 05.09.2005 (BGBl. I S. 2722); Baden-Württemberg: Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg vom 17.12.2015 (GBl. S. 1201); Berlin: Berliner Informationsfreiheitsgesetz – IFG vom 15.10.1999 (GVBl. S. 561);

Bremen: Gesetz über die Freiheit des Zugangs zu Informationen für das Land Bremen (Bremer Informationsfreiheitsgesetz – BremIFG) vom 16.05.2006 (GBl. S. 263); Hamburg: Hamburgisches Transparenzgesetz (HmbTG) vom 19.06.2012 (GVBl. S. 271); Mecklenburg-Vorpommern: Gesetz zur Regelung des Zugangs zu Informationen für das Land Mecklenburg-Vorpommern (Informationsfreiheitsgesetz – IFG M-V) vom 10.07.2006 (GVOBl. S. 566); Nordrhein-Westfalen: Gesetz über die Freiheit des Zugangs zu Informationen für das Land Nordrhein-Westfalen (Informationsfreiheitsgesetz-Nordrhein-Westfalen – IFG NRW) vom 27.11.2001 (GV S. 806); Rheinland-Pfalz: Landestransparenzgesetz (TranspG) vom 17.11.2015 (GVBl. S. 383); Saarland: Saarländisches Informationsfreiheitsgesetz (SIFG) vom 12.07.2006 (ABl. S. 1624);Sachsen-Anhalt: Informationszugangsgesetz Sachsen-Anhalt – IZG LSA vom 29.06.2008 (GVBl. S. 242); Schleswig-Holstein: Informationszugangsgesetz für das Land Schleswig-Holstein vom 19.01.2012 (GVOBl. S. 89). Der Datenschutz und mit ihm die informationelle Selbstbestimmung wurden als Schranken der Informationsansprüche verstanden, die gegeneinander abzuwägen waren. In den einzelnen Informationsfreiheitsgesetzen wurde der Transparenz unterschiedliches Gewicht beigemessen. Daraus glaubten Transparenzprotagonisten, ein Ranking der Gesetze aufstellen zu sollen. Das bedeutet zugespitzt, dass eine gute Bewertung der Transparenz durch eine schlechte Bewertung beim Datenschutz erkauft wird, wenn man sich auf das Verfahren einlässt. Gegen dieses Fehlverständnis muss jedoch Front bezogen werden, weil die Antinomie von Informationsfreiheit und Datenschutz der **Entwicklung der informationellen Selbstbestimmung** nicht gerecht wird.

1.3 Informationelle Selbstbestimmung

1.3.1 Dogmatische Grundlagen

Die informationelle Selbstbestimmung wurde in den zurückliegenden Tätigkeitsberichten schon mehrfach gewürdigt. Danach liegt der informationellen Selbstbestimmung ein (vom Verfassungsgeber) **unbenanntes Grundrecht** zugrunde, das ursprünglich dazu diente, das noch weitgehend unbekannte Datenschutzgrundrecht zu etikettieren. Die geschilderten Konkretisierungen dieses Grundrechts waren nur Momentaufnahmen. Das heutige Verständnis der informationellen Selbstbestimmung geht über diesen Ansatz hinaus. Die informationelle Selbstbestimmung ist als Institut des Verfassungsrechts auf Fortentwicklung angelegt. Die Fortentwicklung sollte dabei nicht ziellos, sondern in geordneten Bahnen verlaufen. Um in diesem Sinn auf die Entwicklung

Einfluss nehmen zu können, ist es hilfreich, die bisherigen Entwicklungslinien noch einmal grob zu skizzieren.

1.3.2
Vorläufer im Schrifttum

Die informationelle Selbstbestimmung ist ein Konstrukt des Bundesverfassungsgerichts. Das Bundesverfassungsgericht wiederum griff Anregungen des Schrifttums auf und setzte sich mit der Kritik aus dem Schrifttum auseinander. Die Entwicklung der informationellen Selbstbestimmung durch das Bundesverfassungsgericht wird daher nur verständlich, wenn die Bezüge zu Äußerungen aus dem Schrifttum mitberücksichtigt werden. So wurden Ausdruck und – in Ansätzen – auch Begriff der informationellen Selbstbestimmung von Autoren entwickelt, die auch als Prozessvertreter im Volkszählungsstreit auftraten. Soweit ersichtlich, wird der Ausdruck erstmals in einem Gutachten verwendet, das Steinmüller dem Bundesminister des Innern erstattete (veröffentlicht als Anhang zu BTDrucks. VI/3826). Dort findet sich auf S. 139 die Aussage: „… muss weiterführend festgestellt werden, dass die allgemeine Handlungsfreiheit das Verfügungs- und damit das Zurückbehaltungsrecht bezüglich aller Individualinformationen umfasst, also als ‚informationelles Selbstbestimmungsrecht' zu verstehen ist." Die nicht näher definierte informationelle Selbstbestimmung wurde als Unterfall der allgemeinen Handlungsfreiheit behandelt. Eine umfassendere Begründung hierfür lieferte Podlech im Alternativkommentar zum Grundgesetz (1. Aufl. 1984, Art. 2 Abs. 1, Rdnr. 45). Nur wer mit einer hinreichend sicheren Prognose überschauen könne, welche ihn betreffenden Informationen in bestimmten Sektoren seiner sozialen Umwelt bekannt seien, konkret, nur wer das Wissen möglicher Kommunikationspartner in etwa abschätzen könne, sei in der Lage, Handlungen in die Zukunft aus eigener Selbstbestimmung zu planen und zu entscheiden. Mit Art. 2 Abs. 1 GG sei eine Rechtsordnung unvereinbar, in der der Bürger nicht wisse könne, wer, was, wann und bei welcher Gelegenheit über ihn wisse. Beide Autoren äußerten sich im Volkszählungsstreit des Bundesverfassungsgerichts. Ihre Argumentation zu den tatsächlichen Voraussetzungen der informationellen Selbstbestimmung wurde vom Bundesverfassungsgericht übernommen. Expressis verbis knüpfte das Bundesverfassungsgericht jedoch an seine eigene Rechtsprechung an.

1.3.3 Volkszählungsurteil

Im Volkszählungsurteil (BVerfGE 65, 1) kreierte das Bundesfassungsgericht das Grundrecht auf informationelle Selbstbestimmung, um den „heutigen und künftigen Bedingungen der automatisierten Datenverarbeitung“ gerecht zu werden. Dabei nutzte es Formulierungen aus dem Schrifttum zur Verknüpfung mehrerer Argumentationsstränge seiner bisherigen Rechtsprechung. **Prüfungsmaßstab** war das in Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das schon in der Mikrozensus-Entscheidung dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung zugewiesen hatte (BVerfGE 27, 344 [(350)]; vgl. auch BVerfGE 120, 274 (321 f.). Aus dem Gedanken der Selbstbestimmung leitete das Bundesverfassungsgericht die Befugnis des Einzelnen ab, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart würden (**Verhaltensfreiheit**). Die individuelle Selbstbestimmung setze voraus, dass es dem Einzelnen möglich sei, sich über vorzunehmende oder zu unterlassende Handlungen frei zu entscheiden (**Entscheidungsfreiheit**). Diese Freiheit habe nicht, wer nicht wisse, welche ihn betreffenden Informationen der sozialen Umwelt bekannt seien. „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer, was, wann und bei welcher Gelegenheit über sie weiß“ (BVerfGE 65, 1, 43). Wer unsicher sei, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben würden, werde in der Regel versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil informierte Bürger Funktionsbedingung einer freiheitlichen demokratischen Grundordnung seien. Während das Bundesverfassungsgericht den Schutzbereich des neugeschaffenen Grundrechts reichlich vage umschrieb, bemühte es sich um präzise Vorgaben bei den Schranken. Danach sei das Grundrecht zwar nicht schrankenlos, jedoch bestünden bei der Beschränkung der informationellen Selbstbestimmung höhere Anforderungen als bei der allgemeinen Handlungsfreiheit. Eingriffe in die informationelle Selbstbestimmung bedürften einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen müsse, der Grundsatz der Verhältnismäßigkeit sei datenschutzspezifisch

auszulegen. Erforderlich sei schließlich die Wahrung des Zweckbindungsgrundsatzes.

1.3.4
Weitere Entwicklung

Stoßrichtung der Rechtsprechung des Bundesverfassungsgerichts war zunächst die Abwehr staatlicher Eingriffe in von der informationellen Selbstbestimmung erfasste Schutzbereiche. Anders als das Schrifttum, das überwiegend nur auf Art. 2 Abs. 1 GG abgestellt hatte, stützte sich das Bundesverfassungsgericht auf Art. 2 Abs. 1 und Art. 1 Abs. 1 GG. Diese Kombination diente ursprünglich vor allem dem Bundesgerichtshof zur Verstärkung der Handlungsfreiheit bei gravierenden Persönlichkeitsrechtsverletzungen. In diesem Zusammenhang entwickelten sich Schutzsphären, die ihren Höhepunkt im „Kernbereich privater Lebensgestaltung" erlangten, der seinerseits unmittelbar durch Art. 1 Abs. 1 GG geschützt wurde. War aber die Menschenwürde der eine Fixpunkt für die Beurteilung, dann musste Art. 2 Abs. 1 GG der zweite Fixpunkt sein. Auf diese Weise entstand eine Abwägungsskala für Eingriffe in das neu benannte Grundrecht der informationellen Selbstbestimmung. Auf dem 17. Wiesbadener Forum Datenschutz 2009 führte der damalige Präsident des Bundesverfassungsgerichts hierzu aus: „Es ist in der Tat so, dass in allen diesen Freiheitsrechten – dem Schutz der Persönlichkeit –, aber auch den speziellen Freiheitsrechten wie dem Schutz der Unverletzlichkeit der Wohnung oder dem Schutz des Telekommunikationsgeheimnisses des Art. 10 GG ein Menschenwürdekern steckt. Sie haben völlig Recht. Im Grunde gilt es nach wie vor, Sphären des Grundrechtsschutzes zu unterscheiden, Herr Professor Dr. Ronellenfitsch. Sie haben es schön ausgedrückt. Je mehr sich der staatliche Eingriff diesem Bereich des Menschenwürdekerns nähert, desto höher werden die Anforderungen an das Gewicht des zu schützenden Rechtsguts" (in: Der Hessische Datenschutzbeauftragte/ Der Präsident des Hessischen Landtags [Hrsg.], Vorgaben des Bundesverfassungsgerichts für die zeitgemäße Datenschutzkultur in Deutschland, 2010, S. 45). Die informationelle Selbstbestimmung ist folglich dynamisch in der ebenfalls dynamisch angelegten Werteordnung des Grundgesetzes zu verstehen.

1.4
Hessische Lösung

Unter Ziff. 2.4.1 wurde die Entwicklung des hessischen Datenschutzrechts zu einer Teilmaterie des Rechts der informationellen Selbstbestimmung geschildert. Die gleiche Entwicklung lediglich aus einem anderen Blickwinkel stellt

die Entwicklung des Hessischen Informationsfreiheitsgesetzes dar. Dieser Entwicklung ging eine intensive rechtliche und rechtspolitische Diskussion voraus, die einen Höhepunkt auf dem 15. Wiesbadener Forum Datenschutz 2006 fand (vgl. Der Hessische Datenschutzbeauftragte/Der Präsident des Hessischen Landtags [Hrsg.], Informationsfreiheit und Datenschutz, 2007). Im Schlusswort zu dieser Veranstaltung führte der Hessische Datenschutzbeauftragte aus: „Die Gesetzgeber spielen sich einen Streich, wenn sie die Chancen für eine informierte Bevölkerung im Interesse der Demokratie nicht nutzen“ (ebd. S. 86). Auch bei anderen Gelegenheiten sprach sich der Hessische Datenschutzbeauftragte häufig für ein hessisches Informationsfreiheitsgesetz aus (vgl. 34. Tätigkeitsbericht, Ziff. 2.1.2.2; 35. Tätigkeitsbericht, Ziff. 1.3.1). In der Stellungnahme zum Gesetzentwurf der Fraktion der SPD für ein hessisches Transparenzgesetz (Hess. TG – LTDrucks. 18/7200) heißt es: „Das Grundgesetz und die Hessische Verfassung schützen den Menschen als kommunikatives Wesen durch ein Bündel geschriebener und ungeschriebener Grundrechte, zu denen auch die Informationsfreiheit zählt. Informationelle Selbstbestimmung impliziert auch das Recht, sich aus allgemein zugänglichen Quellen zu informieren. Aufgabe des Gesetzgebers ist es, solche Quellen zu eröffnen oder zumindest den freien und sicheren Informationsfluss zu gewährleisten. Die Herstellung einer derartigen Informationsfreiheit war schon immer von der Aufgabenstellung des Datenschutzes erfasst.“ Die Erstreckung der informationellen Selbstbestimmung in den Bereich des Informationszugangs verstärkt die Rechtsstellung der Bürgerinnen und Bürger und macht diese nicht zum Mittel zum Zweck der Staatskontrolle. Der hessische Gesetzgeber hat daher davon abgesehen, das Transparenzprinzip als bürgerliches Kontrollinstrument über die Verwaltung heranzuziehen.

2. Grundzüge des Hessischen Informationsfreiheitsgesetzes

Das Hessische Innenministerium hat mit mir an zwei Terminen eine Fortbildungsveranstaltung für die Abteilungsleiterinnen und Abteilungsleiter der hessischen Ministerien durchgeführt, in denen neben dem neuen Datenschutzrecht (insb. DS-GVO) das Informationsrecht gemäß dem Hessischen Informationsfreiheitsgesetz in seinen Grundzügen erläutert wurde.

2.1
Anwendungsbereich

Der grundsätzliche Anspruch gegenüber öffentlichen Stellen auf Zugang hinsichtlich amtlicher Informationen (§ 80 Abs. 1 HDSIG) wird durch das Gesetz rechtlich ausgestaltet. Soweit das Gesetz den Informationszugang eröffnet, handelt es sich bei den amtlichen Informationen dann um allgemein zugängliche Quellen im Sinne von Art. 5 Abs. 1 S. 1 GG. Gänzlich ausgenommen ist der Anspruch auf Informationszugang im Hinblick auf die Polizeibehörden, das Landesamt für Verfassungsschutz, die Landeskartellbehörde, die Regulierungskammer Hessen, die Industrie- und Handelskammern, die Handwerkskammern sowie Notarinnen und Notare, § 81 Abs. 2 HDSIG.

Daneben gibt es gemäß § 81 Abs. 1 HDSIG den Anspruch auf Informationszugang gegenüber bestimmten Stellen nur, soweit nicht – pointiert formuliert – die Hauptfunktion der Stelle betroffen ist. Der Anspruch besteht also nur in Hinblick auf den allgemeinen Verwaltungsbereich bei folgenden Stellen:

– Hessischer Landtag
– Hessischer Rechnungshof
– Hessischer Datenschutzbeauftragter
– Gerichte
– Strafverfolgungs- und Strafvollstreckungsbehörden
– Finanzbehörden
– Universitätskliniken
– Forschungseinrichtungen
– Hochschulen
– Schulen
– Hessischer Rundfunk
– Hessische Landesanstalt für privaten Rundfunk und neue Medien

Eine besondere Regelung hat der Gesetzgeber für die Kommunen vorgesehen (§ 81 Nr. 7). Er überlässt die dortige Geltung des Hessischen Informationsfreiheitsgesetzes den „Kommunalparlamenten“ als freie Selbstverwaltungs-

aufgabe: Es obliegt deren Entscheidung, die Geltung der §§ 80 ff. HDSIG durch Satzung ausdrücklich zu bestimmen.

Das Gesetz eröffnet den Anspruch auf Informationszugang aber nicht nur im Hinblick auf bestimmte Stellen der öffentlichen Hand, sondern gewährt den Anspruch bezogen auf alle öffentlichen Stellen nach Maßgabe von inhaltlichen Kriterien, nämlich besonderer öffentlicher und privater Belange.

2.2
Schutz besonderer öffentlicher und privater Belange

Zugunsten dieser Belange besteht der Anspruch gemäß § 82 HDSIG gänzlich nicht bei Verschlusssachen im Sinne des Hessischen Sicherheitsüberprüfungsgesetzes (Nr. 1) und bei einem Berufs- oder besonderen Amtsgeheimnis unterliegenden Datei- oder Akteninhalten (Nr. 4).

Nicht generell ausgeschlossen ist der Anspruch gemäß § 82 Nr. 2 HDSIG, wonach nämlich jeweils geprüft werden muss, ob das Bekanntwerden von Informationen nachteilige Auswirkungen haben kann auf:

a) inter- und supranationale Beziehungen, die Beziehung zum Bund oder zu einem anderen Land,
b) Belange der äußeren oder öffentlichen Sicherheit,
c) Kontroll-, Vollzugs- oder Aufsichtsaufgaben der Finanz-, Regulierungs-, Sparkassen, Versicherungs- und Wettbewerbsaufsichtsbehörden,
d) den Erfolg eines strafrechtlichen Ermittlungs- oder Strafvollstreckungsverfahrens oder den Verfahrensablauf eines Gerichts-, Ordnungswidrigkeiten- oder Disziplinarverfahrens.

Speziell dem Grundrechtsschutz der Bürgerinnen und Bürger, aber auch dem Grundrechtsschutz juristischer Personen (Art. 19 Abs. 3 GG) dient die Regelung des § 82 Nr. 4 HDSIG, wonach ein Anspruch auf Informationszugang nicht besteht bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- und Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat.

2.3
Datenschutz als Voraussetzung des Informationszugangs

Datenschutz und Informationszugang sind keine voneinander unabhängigen Rechtsgebiete, sondern der Informationszugang setzt die Beachtung des Datenschutzes voraus. Soweit der persönliche Lebensbereich betroffen ist, bestimmt die/der Betroffene, ob und inwieweit ein Anspruch auf Informations-

zugang besteht: Ohne Einwilligung der in ihren Rechten betroffenen Person besteht kein Informationszugang (§ 82 Abs. 4 Nr. 2 HDSIG).

Falls die Einwilligung nicht innerhalb eines Monats nach der Anfrage durch die öffentliche Stelle, von der Informationen begehrt werden, vorliegt, gilt die Einwilligung der/des Betroffenen zum Informationszugang der antragstellenden Person als verweigert (§ 86 S. 2 HDSIG).

Soweit zwar nicht der persönliche Lebensbereich betroffen ist, es aber dennoch um personenbezogene Daten geht, steht der Informationszugang nicht unter dem Einwilligungsvorbehalt des Betroffenen, sondern unter Abwägungsvorbehalt der zuständigen öffentlichen Stelle. Die Entscheidungszuständigkeit verlagert sich in diesem Fall also von dem Betroffenen auf die öffentliche Stelle, die über den Informationszugang zu befinden hat.

Wie zum „Schutz personenbezogener Daten", so die amtliche Überschrift zu § 83 HDSIG, von der öffentlichen Stelle hierbei zu verfahren ist, gibt diese Vorschrift knapp und prägnant vor:

„Der Informationszugang zu personenbezogenen Daten ist nur dann und soweit zulässig, wie ihre Übermittlung an eine nicht öffentliche Stelle zulässig ist."

Auch hier zeigt sich im HDSIG deutlich, dass die Entscheidung des Gesetzgebers, Datenschutz und Informationsfreiheit in einem Gesetz zu regeln, rechtssystematisch konzise ist, denn Datenschutz und Informationszugang sind im HDSIG rechtsdogmatisch miteinander verzahnt:

§ 83 HDSIG verweist nämlich inhaltlich auf § 22 Abs. 2 Nr. 2 HDSIG und bildet zusammen mit dieser Norm eine Verbundbestimmung. Diese verlangt eine Bewertung der berechtigten Interessen des Auskunftsbegehrenden und der schutzwürdigen Interessen des Betroffenen. Damit für diese Bewertung die nötigen Informationen möglichst zur Verfügung stehen, muss der Antragsteller sein Informationsgesuch begründen (§ 85 Abs. 3 HDSIG) und der in seinen Daten Betroffene muss Gelegenheit zur Stellungnahme erhalten, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann (§ 86 S. 1 HDSIG).

2.4
Die Entscheidung über ein Informationsbegehren

Fristen für die Entscheidung

Für die Entscheidung über einen Informationsantrag bestimmt das Gesetz Fristen. Es ist unverzüglich, also ohne schuldhaftes Zögern zu entscheiden, spätestens aber innerhalb eines Monats, bei Drittbeteiligung spätestens innerhalb von drei Monaten nach Eingang eines hinreichend bestimmten

Antrags, § 87 Abs. 1 HDSIG. Die öffentliche Stelle kann diese Fristen um einen Monat verlängern, wenn die Auskunftsgewährung insbesondere wegen der Komplexität des Informationsersuchens nicht eingehalten werden kann, § 87 Abs. 4 HDSIG; also kann bei Informationsersuchen ohne Drittbeteiligung die Frist auf zwei Monate verlängert werden, im Fall von Drittbeteiligung auf vier Monate.

Über eine solche Fristverlängerung muss die antragstellende Person unter Angabe der maßgeblichen Gründe dann aber schriftlich informiert werden (§ 87 Abs. 4 S. 2 HDSIG).

Bekanntgabe und Vollziehung der Entscheidung

Soweit dem Informationsantrag stattgegeben wird, müssen die Informationen innerhalb der für die Entscheidung geltenden Fristen zugänglich gemacht werden, § 87 Abs. 2 HDSIG. Sind durch eine dem Antrag stattgebende Entscheidung der öffentlichen Stelle andere Personen in ihren Rechten betroffen, müssen diese die Möglichkeit haben, gegen die Entscheidung der öffentlichen Stelle gerichtlich vorzugehen, um die Rechtmäßigkeit der getroffenen Entscheidung überprüfen lassen zu können. Daher darf in einem solchen Fall von Drittbetroffenheit Informationszugang erst dann gewährt werden, wenn die Entscheidung der öffentlichen Stelle, also dieser Verwaltungsakt, unanfechtbar/bestandskräftig geworden ist, das heißt, falls kein Rechtsbehelf eingelegt wird, einen Monat nach Bekanntgabe der Entscheidung mit Rechtsbehelfsbelehrung und ein Jahr nach Bekanntgabe der Entscheidung ohne Rechtsbehelfsbelehrung (§§ 58, 74 VwGO).

Es ist evident, dass im Fall einer dem Informationsersuchen stattgebenden Entscheidung eine Rechtsbehelfsbelehrung geboten ist, um die Informationsgewährung nicht unnötig zu verzögern.

Weil bei Informationen mitunter der Zeitpunkt der Bekanntgabe eine ausschlaggebende Rolle spielen kann, sieht § 87 Abs. 2 S. 2 im Fall der Anordnung der sofortigen „Vollstreckung“ (richtig: „Vollziehung“: § 80 Abs. 1 Nr. 4 VwGO) der Verwaltungsentscheidung die Gewährung des Informationszugangs schon nach zwei Wochen ab dem Zeitpunkt der Bekanntgabe der Anordnung der sofortigen Vollziehung an den Dritten vor, um dessen Daten es geht. Der Dritte hat wiederum in dieser Zeitspanne die Möglichkeit, um vorläufigen Rechtsschutz beim Verwaltungsgericht zu ersuchen (§ 80 Abs. 5 VwGO).

Wird der beantragte Informationszugang von der öffentlichen Stelle hingegen ganz oder teilweise abgelehnt, muss diese Entscheidung von ihr schriftlich begründet werden. Und sie hat mitzuteilen, ob und wann ein Informationsanspruch ganz oder teilweise zu einem späteren Zeitpunkt voraussichtlich

möglich sein könnte (§ 87 Abs. 3 HDSIG). Gegen die Entscheidung der öffentlichen Stelle über die Informationsgewährung findet ein Vorverfahren nicht statt, sondern es muss unmittelbar verwaltungsgerichtlicher Rechtsschutz in Anspruch genommen werden, § 87 Abs. 5 HDSIG. Hinzu kommt die Möglichkeit, sich an den Hessischen Informationsfreiheitsbeauftragten zu wenden, § 89 HDSIG. Kurz gefasst ist es gemäß dieser Vorschrift Aufgabe und Befugnis der/des Hessischen Informationsfreiheitsbeauftragten, die Umsetzung des Informationsfreiheitsgesetzes zu unterstützen und zu kontrollieren. Daneben ist die/der Beauftragte für Informationsfreiheit selbst eine öffentliche Stelle, die dem Informationszugang (teilweise) unterliegt.

3. Bisherige Umsetzung

3.1 Informationsanträge an den Hessischen Beauftragten für Informationsfreiheit

Mehrere Eingaben betrafen Unterlagen der Schufa Holding AG (Schufa). Da meine Behörde die für dieses Unternehmen zuständige Datenschutzaufsichtsbehörde ist (Unternehmenssitz ist Wiesbaden) und da dieses Unternehmen mit Blick auf seine Datenverarbeitung, insbesondere die Bewertung der Kreditwürdigkeit der Bürgerinnen und Bürger (Scorewert), datenschutzaufsichtsbehördlich von großer Relevanz ist, sind in meinem Haus wichtige Unterlagen, die die Auskunftei betreffen, vorhanden.

Die Eingeber wollten u. a. Gutachten, die die Schufa Holding AG in Auftrag gegeben hatte und die sich mit deren Scoringverfahren befassen, zur Verfügung gestellt bekommen. Ich habe die Informationsbegehren zurückgewiesen, denn die Unterlagen betreffen nicht meinen allgemeinen Verwaltungsbereich, sondern sind Gegenstand meiner datenschutzaufsichtsbehördlichen Prüfung. Insoweit gibt es keinen Informationszugang, § 81 Abs. 1 Nr. 3 HDSIG (näher erläuternd die Begründung des Regierungsentwurfs zu § 81, LTDrucks. 19/5728, S. 149).

Würde es diese spezielle Regelung in § 81 Abs. 1 Nr. 3 HDSIG nicht geben, hätte sich mit Blick auf § 82 Nr. 4 HDSIG die schwierige Frage gestellt, wie weit bei der Beurteilung der Kreditwürdigkeit das Geschäftsgeheimnis der Schufa reicht.

Die Beurteilung der Reichweite von Betriebs- und Geschäftsgeheimnissen ist eine der heikelsten Fragestellungen, die im Kontext der Informationsfreiheit anfallen. Am plastischsten zeigt das die im Sommer 2018 bekannt gegebene Entscheidung des Europäischen Gerichtshofs (betr. Bundesanstalt für Finanzdienstleistungsaufsicht/Baumeister), die den Abschluss einer über zehnjährigen gerichtlichen Auseinandersetzung betreffend die Auskunftsverpflichtung der BaFin gegenüber einem Informationsbegehrenden bildete. Der Kläger war durch ein Finanzunternehmen (Phoenix Kapitaldienst GmbH), das der Aufsicht der BaFin unterstand, mittels eines betrügerischen sogenannten „Schneeballsystems“ geschädigt worden (EuGH, Urt. v. 19.06.2018 – C - 15/16; NVwZ 2018/1368 ff. mit Anm. B. Huber).

Ein solcher Rechtsstreit wäre gegen den Hessischen Informationsfreiheitsbeauftragen deshalb undenkbar, weil hinsichtlich seiner Behörde eben nur allgemeine Verwaltungsaufgaben vom Informationszugang betroffen sind. Genau wegen dieser gesetzlichen Vorgabe habe ich anderseits beispielswei-

se Informationsanfragen unverzüglich beantwortet, die die Aktenverwaltung meiner Behörde/Zusammenarbeit mit dem Hessischen Staatsarchiv oder auch den Personalaufwand meiner Behörde für das Sachgebiet „Videoüberwachung“ betrafen.

3.2
Informationsanträge an andere öffentliche Stellen

Soweit Informationsanträge an andere Stellen gerichtet wurden, ist mir das nur dann bekannt geworden, wenn im Verfahren (häufig auch telefonisch) Beschwerden oder Anfragen seitens der Antragstellerinnen/Antragsteller oder seitens der betroffenen öffentlichen Stellen an mich gerichtet worden sind.

Informationsanträge an Kommunen

Mehrfach ging es um Informationsanträge gegenüber Kommunen. Selten hatten Kommunen auf einen Informationsantrag überhaupt nicht reagiert. In aller Regel wurde den Antragstellern von der Kommune mitgeteilt, dass das Informationsfreiheitsgesetz auf kommunaler Ebene nur dann gilt, wenn das die Kommunalvertretung durch Satzung so beschlossen hat (§ 81 Abs. 1 Nr. 7 HDSIG). Soweit Kommunen ausnahmsweise nicht auf einen Antrag antworteten, kam es zu Eingaben bei mir, die ich dann unter Hinweis auf diese Rechtslage beantwortet habe.

Die in diesem Zusammenhang von Eingebern, aber insbesondere auch von Informationsfreiheitsbeauftragen geäußerte harsche Kritik, es sei der Informationsfreiheit und dem damit verbundenen Demokratieprinzip abträglich, die Informationsfreiheit nicht den Kommunen durch Gesetz auferlegt zu haben, überzeugt mich in ihrer Schärfe nicht. Im Gegenteil ist es gerade auch ein Ausdruck von Demokratie, die Einführung der Informationsfreiheit auf kommunaler Ebene der kommunalen Volksvertretung zu überlassen. Dass mir bislang bis auf die großen Städte Hessens (Frankfurt am Main, Wiesbaden, Kassel, Marburg) keine Kommune bekannt geworden ist, die die Anwendbarkeit des Informationsfreiheitsgesetzes für ihren Bereich zu beschließen beabsichtigt, zeigt ja auch Distanz der kommunalen Volksvertretungen zu den Informationsfreiheitsregelungen im kommunalen Bereich.

Vor diesem Hintergrund gehe ich generell davon aus, dass die Kommunen hinsichtlich der Anwendbarkeit des Informationsfreiheitsgesetzes eher zurückhaltend sein werden. Sie sind ja auch im Fall dieser fehlenden Anwendbarkeit nicht gehindert, Informationsanfragen von Bürgerinnen und Bürgern im Wege freier Selbstverwaltung zu beantworten.

Informationsanträge insbesondere an Ministerien

Das Schwergewicht meiner Tätigkeit auf dem Gebiet der Informationsfreiheit betraf die Abstimmung mit den Ministerien beim Umgang mit Informationsanträgen. Im Bereich der Informationsfreiheit ist für diese Abstimmung zwischen Antragstellerinnen/Antragstellern, den Informationsfreiheitsbeauftragten und den betroffenen öffentlichen Stellen der Begriff „Vermittlung“ üblich geworden. Auffallend ist in diesem Zusammenhang, dass ich oft Beschwerden bereits dann bekam, wenn die einmonatige Standardfrist für die Beantwortung von Informationsersuchen um einen Tag überschritten war (das betrifft besonders Eingaben, für die das Internet-Portal „fragdenstaat“ genutzt wird). Diese Vorgehensweise erscheint einerseits kleinlich; aber andererseits lässt sich dem durch eine entsprechende Zwischennachricht seitens der betroffenen öffentlichen Stelle vorbeugen, § 87 Abs. 4 HDSIG. Genau eine solche Zwischennachricht wurde von den öffentlichen Stellen aber manchmal nicht gegeben, und es ist zu hoffen, dass sich das im Laufe der Zeit bessert.

Oftmals übersahen allerdings die Antragsteller, dass bei Drittbetroffenheit statt einer 1-Monats- stattdessen eine 3-Monatsfrist gilt, § 87 Abs. 3 HDSIG, und dass die Frist auch erst zu laufen beginnt „nach Eingang des hinreichend bestimmten Antrags“, § 87 Abs. 1 HDSIG.

Wichtiger als das Vorstehende ist allerdings die für mich erfreuliche erste Bilanz, dass mir bislang kein Fall bekannt geworden ist, in dem eine Auskunft bei einem korrekt gestellten Antrag rechtswidrig nicht gegeben wurde (jedenfalls nicht nach meiner Beratung). Dies widerspiegelnd gibt es in Hessen bislang auch keine Anzeichen dafür, dass auf dem Gebiet der Informationsfreiheit ein verwaltungsgerichtliches Verfahren anhängig werden könnte, um streitige Fragen rechtsverbindlich zu klären.

Die Kosten – eine umfangreiche wissenschaftliche Anfrage beim Kultusministerium

Mitte 2018 reichte ein Professor der Universität Erfurt und des Wissenschaftszentrums Berlin für Sozialforschung bundesweit bei den Kultusministerien einen sehr umfangreichen Fragenkatalog ein, der zahlreiche Aspekte des Themas „Private Ersatzschulen“ betraf. Die Fragen zu beantworten war nach Aussage des Kultusministeriums personalaufwändig und zeitintensiv. Dem Fragesteller wurden deshalb von anderen Bundesländern teils vierstellige Gebühren in Rechnung gestellt.

Hinsichtlich einiger Verfahrensfragen und insbesondere wegen des Kostenaspekts hat sich das Kultusministerium mit mir abgestimmt. Dem Antragsteller wurden Gebühren in Höhe von 600 EUR gemäß dem Verwaltungskostenver-

zeichnis zum HDSIG in Rechnung gestellt. Das ist zwar der Höchstbetrag, den das Gesetz für Auskunftsgebühren im Rahmen der Informationsfreiheit vorsieht, aber immer noch vergleichsweise mäßig.

§ 88 HDSIG sieht ausdrücklich vor, dass die Gebühren auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen sind, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs abgehalten werden. Ganz dementsprechend bestimmt die Vorschrift die Informationsfreiheit unterstützend denn auch einleitend, dass die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort ohnehin kostenfrei sind.

Materialien

1. Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

1.1
Entschließungen der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 26.04.2018

Facebook-Datenskandal – Neues Europäisches Datenschutzrecht bei Sozialen Netzwerken durchsetzen!

Im März 2018 wurde in der Öffentlichkeit bekannt, dass über eine von November 2013 bis Mai 2015 mit Facebook verbundene App nach Angaben des Unternehmens Daten von 87 Millionen Nutzern weltweit, davon 2,7 Millionen Europäern und etwa 310.000 Deutschen erhoben und an das Analyseunternehmen Cambridge Analytica weitergeben wurden. Dort wurden sie offenbar auch zur Profilbildung für politische Zwecke verwendet.

Aus diesem Anlass hat der national zuständige Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Bußgeldverfahren gegen Facebook eingeleitet. Er steht dabei in engem Austausch mit seinen europäischen Kollegen, insbesondere mit dem Information Commissioner's Office in Großbritannien sowie der Artikel 29-Gruppe. Der Datenskandal um Facebook und Cambridge Analytica wirft ein Schlaglicht auf den Umgang mit Millionen Nutzerdaten. Zudem dokumentieren die Vorgänge um Cambridge Analytica, dass Facebook über Jahre hinweg den Entwicklern von Apps den massenhaften Zugriff auf Daten von mit den Verwendern der Apps befreundeten Facebook-Nutzenden ermöglicht hat. Das geschah ohne eine Einwilligung der Betroffenen. Tatsächlich ist der aktuell diskutierte Fall einer einzelnen App nur die Spitze des Eisbergs. So geht die Zahl der Apps, die das Facebook-Login-System nutzen, in die Zehntausende. Die Zahl der davon rechtswidrig betroffenen Personen dürfte die Dimension des Cambridge Analytica-Falls in dramatischer Weise sprengen und dem Grunde nach alle Facebook-Nutzenden betreffen. Das Vorkommnis zeigt zudem die Risiken für Profilbildung bei der Nutzung sozialer Medien und anschließendes Mikrotargeting, das offenbar zur Manipulation von demokratischen Willensbildungsprozessen eingesetzt wurde.

Die Datenschutzkonferenz fordert aus diesen offenbar massenhaften Verletzungen von Datenschutzrechten Betroffener folgende Konsequenzen zu ziehen:

– Soziale Netzwerke müssen ihre Geschäftsmodelle auf die neuen europäischen Datenschutzregelungen ausrichten und ihrer gesellschaftliche Verantwortung nachkommen. Dazu gehört auch, angemessene Vorkehrungen gegen Datenmissbrauch zu treffen.
– Facebook muss den wahren Umfang der Öffnung der Plattform für App-Anbieter in den Jahren bis 2015 offenlegen und belastbare Zahlen der eingestellten Apps sowie der von dem Facebook-Login-System betroffenen Personen nennen. Ferner gilt es Betroffene über die Rechtsverletzungen zu informieren.
– In Zukunft muss Facebook sicherstellen, dass die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) rechtskonform umgesetzt werden: Die Vorstellung von Facebook zur Einführung der automatischen Gesichtserkennung in Europa lässt erhebliche Zweifel aufkommen, ob das Zustimmungsverfahren mit den gesetzlichen Vorgaben insbesondere zur Einwilligung vereinbar ist. Wenn Facebook die Nutzenden dazu drängt und es ihnen wesentlich leichter macht, der biometrischen Datenverarbeitung zuzustimmen, als sich ihr zu entziehen, führt dies zu einer unzulässigen Beeinflussung des Nutzers.
– Die Reaktionen auf datenschutzwidriges Verhalten sind dabei nicht allein auf den Vollzug des Datenschutzrechts beschränkt, sondern betreffen auch das Wettbewerbs-und Kartellrecht. Die Forderung nach einer Entflechtung des Facebook-Konzerns wird in dem Maße zunehmen, wie sich dieser durch die systematische Umgehung des Datenschutzes wettbewerbswidrige Vorteile auf dem Markt digitaler Dienstleistungen zu verschaffen versucht. Es bedarf europäischer Initiativen, um monopolartige Strukturen im Bereich der sozialen Netzwerke zu begrenzen und Transparenz von Algorithmen herzustellen.

Weil Datenverarbeitungsprozesse zunehmend komplexer und für Betroffene intransparenter werden, kommt der Datenschutzaufsicht eine elementare Rolle zu. Ihre fachliche Expertise ist gefragt, sie muss organisatorisch und personell in der Lage sein, beratend und gestaltend tätig zu sein. Ein starkes Datenschutzrecht und effektive Aufsichtsbehörden vermindern gemeinsam die Risiken für die Bürgerinnen und Bürger in der digitalen Gesellschaft. Sollten Facebook und andere soziale Netzwerke nicht bereit sein, den europäischen Rechtsvorschriften zum Schutz der Nutzenden nachzukommen, muss dies konsequent durch Ausschöpfung aller vorhandenen aufsichtsbehördlichen Instrumente auf nationaler und europäischer Ebene geahndet werden.

1.2
Entschließungen der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 26.04.2018

Zuverlässigkeitsüberprüfungen bei öffentlichen und privaten Veranstaltungen nur im erforderlichen Maß und nach einem rechtsstaatlichen und transparenten Verfahren

Zunehmend werden im Rahmen von öffentlichen und privaten Veranstaltungen Personen, die in unterschiedlichen Funktionen auf einem Veranstaltungsgelände tätig werden wollen oder sonst Zutritt zu Sicherheitszonen begehren (beispielsweise Anwohner), durch Sicherheitsbehörden auf ihre Zuverlässigkeit überprüft. Auch bei privaten Veranstaltungen fordern die Polizeien die Veranstalter bisweilen dazu auf, dafür zu sorgen, dass alle im Rahmen der Veranstaltung Tätigen einer solchen Prüfung unterzogen werden. In den meisten Fällen ist alleinige Grundlage für diese Maßnahmen immer noch die Einwilligung der Betroffenen.

Bereits vor mehr als zehn Jahren haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 25./26. Oktober 2007 darauf hingewiesen, dass allein die Einwilligung der Betroffenen in eine Zuverlässigkeitsüberprüfung keine legitimierende Grundlage für solche tiefen Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen kann. Die wiederholten Forderungen nach Schaffung gesetzlicher Grundlagen haben seitdem die Gesetzgeber nur weniger Bundesländer aufgegriffen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert die Gesetzgeber und die Verantwortlichen deshalb erneut nachdrücklich auf, für ein rechtsstaatliches und transparentes Verfahren solcher Zuverlässigkeitsüberprüfungen zu sorgen, das auf das absolut erforderliche Maß beschränkt bleibt, sowohl was den Umfang der Überprüfung als auch den betroffenen Personenkreis betrifft. Dabei sind insbesondere folgende Rahmenbedingungen zu beachten:

Zuverlässigkeitsüberprüfungen nur aufgrund einer spezifischen Rechtsgrundlage

Die Gesetzgeber werden aufgefordert, bereichsspezifische Rechtsgrundlagen zu schaffen, die den Grundsatz der Verhältnismäßigkeit beachten und aus denen sich die Voraussetzungen und der Umfang der Überprüfungen klar und für die Bürgerinnen und Bürger erkennbar ergeben.

Zuverlässigkeitsüberprüfungen nur im erforderlichen Maß

Anwendung, Umfang, Kreis der betroffenen Personen und die Datenverarbeitung sind auf das Erforderliche zu beschränken. Generell dürfen Zuverlässigkeitsüberprüfungen nur bei solchen Veranstaltungen eingesetzt werden, die aufgrund ihrer spezifischen Ausprägung infolge einer belastbaren Gefahrenprognose als besonders gefährdet bewertet werden. Korrespondierend müssen die personenbezogenen Daten, die in den zum Abgleich herangezogenen Dateien und Informationssystemen gespeichert sind, nicht nur eine ausreichende Qualität haben, es dürfen auch nur hinreichend gewichtige Delikte in die Überprüfung einbezogen werden. Zudem müssen die Kriterien, die zur Annahme von Sicherheitsbedenken führen, einen konkreten Bezug zu den abzuwehrenden Gefahren haben.

Zuverlässigkeitsüberprüfungen nur in einem transparenten Verfahren

Die Rechte und Freiheiten der betroffenen Personen müssen durch ein transparentes Verfahren gewährleistet werden. Dazu müssen insbesondere Anhörungsrechte der betroffenen Personen rechtlich verankert werden. Im praktischen Verfahren kann im Einzelfall auch die Einrichtung einer Clearingstelle sinnvoll sein. Zudem sollten zumindest die Datenschutzbeauftragten der Verantwortlichen frühzeitig vorab beteiligt werden, damit eine datenschutzrechtliche Beratung für eine datensparsame Ausgestaltung und Beschränkung des konkreten Verfahrens stattfinden kann.

1.3 Entschließungen der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 06.06.2018

Die Zeit der Verantwortungslosigkeit ist vorbei: EuGH bestätigt gemeinsame Verantwortung von Facebook und Fanpage-Betreibern

Die unabhängigen Datenschutzbehörden des Bundes und der Länder begrüßen das Urteil des Europäischen Gerichtshofs (EuGH) vom 5. Juni 2018, das ihre langjährige Rechtsauffassung bestätigt.

Das Urteil des EuGH zur gemeinsamen Verantwortung von Facebook und den Betreibern einer Fanpage hat unmittelbare Auswirkungen auf die Seitenbetreiber. Diese können nicht mehr allein auf die datenschutzrechtliche Verantwortung von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Nutzenden ihrer Fanpage.

Dabei müssen sie die Verpflichtungen aus den aktuell geltenden Regelungen der Datenschutz-Grundverordnung (DS-GVO) beachten. Zwar nimmt das Urteil Bezug auf die frühere Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, doch die vom EuGH festgestellte Mitverantwortung der Seitenbetreiber erstreckt sich auf das jeweils geltende Recht, insbesondere auf die in der DS-GVO festgeschriebenen Rechte der Betroffenen und Pflichten der Verarbeiter.

Im Einzelnen ist Folgendes zu beachten:

– Wer eine Fanpage besucht, muss transparent und in verständlicher Form darüber informiert werden, welche Daten zu welchen Zwecken durch Facebook und die Fanpage-Betreiber verarbeitet werden. Dies gilt sowohl für Personen, die bei Facebook registriert sind, als auch für nicht registrierte Besucherinnen und Besucher des Netzwerks.
– Betreiber von Fanpages sollten sich selbst versichern, dass Facebook ihnen die Informationen zur Verfügung stellt, die zur Erfüllung der genannten Informationspflichten benötigt werden.
– Soweit Facebook Besucherinnen und Besucher einer Fanpage durch Erhebung personenbezogener Daten trackt, sei es durch den Einsatz von Cookies oder vergleichbarer Techniken oder durch die Speicherung der IP-Adresse, ist grundsätzlich eine Einwilligung der Nutzenden erforderlich, die die Anforderung der DS-GVO erfüllt.
– Für die Bereiche der gemeinsamen Verantwortung von Facebook und Fanpage-Betreibern ist in einer Vereinbarung festzulegen, wer von ihnen welche Verpflichtung der DS-GVO erfüllt. Diese Vereinbarung muss in wesentlichen Punkten den Betroffenen zur Verfügung gestellt werden, damit diese ihre Betroffenenrechte wahrnehmen können.

Für die Durchsetzung der Datenschutzvorgaben bei einer Fanpage ist die Aufsichtsbehörde zuständig, die für das jeweilige Unternehmen oder die Behörde zuständig ist, die die Fanpage betreibt. Die Durchsetzung der Datenschutzvorgaben im Verantwortungsbereich von Facebook selbst obliegt primär der irischen Datenschutzaufsicht im Rahmen der europäischen Zusammenarbeit.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des EuGH dringender Handlungsbedarf für die Betreiber von Fanpages besteht. Dabei ist nicht zu verkennen, dass die Fanpage-Betreiber ihre datenschutzrechtlichen Verantwortung nur erfüllen können, wenn Facebook selbst an der Lösung mitwirkt und ein datenschutzkonformes Produkt anbietet, das die Rechte der Betroffenen wahrt und einen ordnungsgemäßen Betrieb in Europa ermöglicht.

1.4
Entschließungen der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 07.11.2018

Der Vorschlag der EU-Kommission für eine E-Evidence-Verordnung führt zum Verlust von Betroffenenrechten und verschärft die Problematik der sog. Vorratsdatenspeicherung

Mit ihrem Vorschlag für eine E-Evidence-Verordnung (Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen (COM (2018) 225 final)) möchte die EU-Kommission eine Alternative zum förmlichen Rechtshilfeverfahren schaffen und den Ermittlungsbehörden einen schnelleren Zugang zu Kommunikationsdaten ermöglichen. Die Strafverfolgungsbehörden der EU-Mitgliedstaaten sollen die Befugnis erhalten, Anbieter von Telekommunikations- und Internetdienstleistungen in anderen Mitgliedstaaten der EU und auch in Staaten außerhalb der EU (Drittstaaten) unmittelbar zur Herausgabe von Bestands-, Zugangs-, Transaktions- und Inhaltsdaten zu verpflichten.

Die DSK weist hierzu auf die kritische Stellungnahme des Europäischen Datenschutzausschusses hin (https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-commission-proposals-european-production-and_de). Diese stellt bereits das Vorliegen einer Rechtsgrundlage in Frage. Mit Besorgnis sieht die DSK vor allem auch die vorgeschlagene Abkehr vom Grundsatz der doppelten bzw. beiderseitigen Strafbarkeit.

Erstmals im Bereich der internationalen Zusammenarbeit in Strafsachen soll die Herausgabe von Daten nicht mehr davon abhängig sein, ob die verfolgte Tat dort, wo die Daten ersucht werden, überhaupt strafbar ist. Im Ergebnis könnten Unternehmen mit Sitz in Deutschland also zur Herausgabe von Daten an Ermittlungsbehörden in anderen EU-Mitgliedstaaten verpflichtet werden, obwohl die verfolgte Tat in Deutschland überhaupt keine Straftat ist. Das könnte zum Beispiel ein in Deutschland erlaubter Schwangerschaftsabbruch sein oder eine politische Meinungsäußerung, wenn diese im ersuchenden Staat strafbewehrt ist.

Zu befürchten ist hierbei auch, dass Drittstaaten die Regelung der EU als Blaupause für eigene Regelungen heranziehen werden. Provider in EU-Mitgliedstaaten würden sich dann vermehrt Herausgabeanordnungen von Drittstaaten ausgesetzt sehen, mit denen möglicherweise Straftaten aus einer völlig anderen Rechtstradition verfolgt werden.

Kritisch sieht die DSK auch, dass im Regelfall jegliche Information und Beteiligung der Justizbehörden des Staates, in dem der Provider seinen

Sitz hat, unterbleibt und damit ein wichtiges verfahrensrechtliches Korrektiv fehlt. Ob die Rechtmäßigkeit eines Ersuchens überprüft wird, hängt im vorgeschlagenen Verfahren ausschließlich vom Verhalten der Provider ab. Nur wenn sich das Unternehmen weigert, Daten zu übermitteln, muss der ersuchende Staat bei den Behörden vor Ort um Vollstreckungshilfe bitten. Nur dann können diese noch in das Verfahren eingreifen. Werden Daten herausgegeben, erlangen die zuständigen Justizbehörden hiervon jedoch keine Kenntnis. Der Vorschlag sieht keine Informationspflicht gegenüber den Behörden am Sitz des Unternehmens vor. Provider verfolgen aber in der Regel wirtschaftliche Interessen und unterliegen in ihren Entscheidungen anderen Verpflichtungen als die Justizbehörden Hierdurch werden Betroffene deutlich schlechter gestellt.

Provider als Adressaten eines Ersuchens sehen sich künftig nicht mehr den Justizbehörden des eigenen Staates gegenüber, sondern müssen sich mit den Behörden des anordnenden Staates auseinandersetzen. Den Betroffenen wiederum steht, wenn überhaupt, nur ein Rechtsbehelf im ersuchenden Mitgliedstaat zu, dessen Rechtsordnung ihnen in der Regel aber fremd ist.

Ein besonderes Verfahren ist vorgesehen, wenn sich Provider mit Sitz in Drittstaaten darauf berufen, dass die angeordnete Übermittlung gegen das dortige Recht verstößt. Für diesen Fall sieht der Vorschlag eine gerichtliche Überprüfung im anordnenden Staat vor. Wenn das Gericht zu der Auffassung gelangt, dass tatsächlich ein Rechtskonflikt vorliegt, muss es die zuständigen Behörden im Zielstaat der Anordnung beteiligen. Das Ergebnis der Konsultation ist für das Gericht verbindlich. Diese Regelung ist ausdrücklich zu begrüßen. Denn auch hier wird eine Blaupause geschaffen für die Frage, welche Rechte europäische Unternehmen in der umgekehrten Situation haben sollten, wenn sie aus Drittstaaten auf der Grundlage von deren Gesetzen (wie z. B. US-Cloud-Act) zu einer Übermittlung verpflichtet werden und welche Verbindlichkeit eine Konsultation der zuständigen Behörden in Europa für Gerichte in Drittstaaten haben sollte.

Besonders kritisch ist jedoch, dass in Deutschland Telekommunikationsdienstleister verpflichtet sind, u. a. sämtliche Verkehrsdaten für zehn Wochen zu speichern. Aus diesen Daten lassen sich genaue Schlüsse auf das Privatleben der Betroffenen, insbesondere deren Kontakt- und Interessenprofil ziehen. Die Problematik dieser sog. Vorratsdatenspeicherung verschärft sich deutlich, wenn ausländische Strafverfolgungsbehörden einen direkten Zugriff auf derartige Informationen erhalten.

Die DSK appelliert daher an alle im Gesetzgebungsverfahren Beteiligten, den Vorschlag für eine E-Evidence-Verordnung zu stoppen!

2. Beschlüsse der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

2.1
Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 05.09.2018

Ablehnung der Behandlung durch Ärztinnen und Ärzte bei Weigerung der Patientin oder des Patienten, die Kenntnisnahme der Informationen nach Art. 13 DSGVO durch Unterschrift zu bestätigen

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sprechen sich dagegen aus, dass Ärztinnen und Ärzte oder andere Angehörige von Gesundheitsberufen die Behandlung ablehnen oder die Verweigerung der Behandlung androhen, wenn die Patientin oder der Patient die Informationen nach Art. 13 DSGVO nicht mit ihrer oder seiner Unterschrift versieht. Eine solche Praxis ist nicht mit der DSGVO vereinbar. Die Informationspflicht nach Art. 13 DSGVO bezweckt lediglich, dass der Patientin bzw. dem Patienten die Gelegenheit gegeben wird, die entsprechenden Informationen einfach und ohne Umwege zu erhalten. Sie oder er muss diese jedoch nicht zur Kenntnis nehmen, wenn sie oder er dies nicht möchte. Um seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachzukommen, kann der Verantwortliche das Aushändigen der Information vermerken oder einen konkreten Verfahrensablauf betreffend die Umsetzung der Informationspflicht dokumentieren, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.

2.2
Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 05.09.2018

Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien

Die Konferenz nimmt das Ergebnis der Beratungen des Arbeitskreises Grundsatzfragen des Datenschutzes zur Kenntnis und empfiehlt für die weitere Rechtspraxis, die im Folgenden aufgeführten Positionierungen bei der Tätigkeit als Aufsichtsbehörde zu Grunde zu legen:

1. Soweit Datenverarbeitungen von Parlamenten (auch deren Organe einschließlich der Abgeordneten) den parlamentarischen Kerntätigkeiten zuzuordnen sind, findet die DSGVO keine Anwendung.
2. Parlamente (auch deren Organe einschließlich der Abgeordneten) unterliegen bei der Ausübung originär parlamentarischer Kerntätigkeiten nur

dann datenschutzrechtlichen Vorgaben und der Aufsicht der Aufsichtsbehörde, wenn sich dies aus einer klaren gesetzlichen Regelung ergibt.

3. Die Einordnung von Tätigkeiten der Parlamente (auch deren Organe einschließlich der Abgeordneten) als verwaltende und fiskalische in Abgrenzung zur parlamentarischen Kerntätigkeit bedarf jeweils einer Bewertung im Einzelfall.
4. Soweit keine gesetzlichen Grundlagen für die parlamentarische Kerntätigkeit bestehen, wäre eine Datenschutzordnung des Parlaments zu empfehlen, die sich an der DSGVO orientieren sollte. Eine Beratung durch die Aufsichtsbehörde sollte in jedem Fall unbenommen bleiben.
5. Parteien als nicht-öffentliche Stellen sind grundsätzlich Normadressaten der DSGVO und unterliegen damit der Aufsicht der Aufsichtsbehörden. Eine mögliche Berücksichtigung ihres besonderen Status im Rahmen der Gesetzesanwendung bleibt unberührt.

2.3
Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 05.09.2018

Zu Facebook-Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-201/16, entschieden, dass eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage –ergeben. Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden. Seit dem Urteil des EuGH sind drei Monate vergangen. Zwar hat Facebook einige Änderungen in seinem Angebot – zum Beispiel bezüglich der Cookies –vorgenommen, doch weiterhin werden auch bei Personen, die keine Facebook-Nutzerinnen und Nutzer sind, Cookies mit Identifikatoren gesetzt, jedenfalls, wenn sie über die bloße Startseite einer Fanpage hinaus dort einen Inhalt aufrufen. Auch werden nach wie vor die Fanpage-Besuche von Betroffenen nach bestimmten, teilweise voreingestellten Kriterien im Rahmen einer sogenannten Insights-Funktion von Facebook ausgewertet und den Betreiberinnen und Betreibern zur Verfügung gestellt. Der EuGH hat unter anderem hervorgehoben, dass „die bei Facebook unterhaltenen Fanpages auch von Personen besucht werden können, die keine

Facebook-Nutzer sind und somit nicht über ein Benutzerkonto bei diesem sozialen Netzwerk verfügen. In diesem Fall erscheint die Verantwortlichkeit des Betreibers der Fanpage hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen der Fanpage durch Besucher automatisch die Verarbeitung ihrer personenbezogenen Daten auslöst." Offizielle Verlautbarungen vonseiten Facebooks, ob und welche Schritte unternommen werden, um einen rechtskonformen Betrieb von Facebook-Fanpages zu ermöglichen, sind bisher ausgeblieben. Eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) wurde bislang nicht zur Verfügung gestellt. Die deutschen Datenschutzaufsichtsbehörden wirken daher auf europäischer Ebene auf ein abgestimmtes Vorgehen gegenüber Facebook hin. Auch Fanpage-Betreiberinnen und -Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO ist der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten wird, rechtswidrig. Daher fordert die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Fanpages erfüllt werden. Dazu gehören insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellen. Eine gemeinsame Verantwortlichkeit bedeutet allerdings auch, dass Fanpage-Betreiberinnen und -Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem können Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DSGVO). Insbesondere die im Anhang aufgeführten Fragen müssen deshalb sowohl von Facebook als auch und von Fanpage-Betreiberinnen und -Betreibern beantwortet werden können.

Anhang: Fragenkatalog

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Art. 26 Abs. 1 DSGVO)
2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Art. 13 und 14 DSGVO nachkommt?
3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?

4. Wie stellen Sie sicher, dass die Betroffenenrechte (Art. 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Art. 17 DSGVO, auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, auf Widerspruch nach Art. 21 DSGVO und auf Auskunft nach Art. 15 DSGVO?
5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?
6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstaufruf einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?
7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Art. 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

2.4
Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26.04.2018

Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. c Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein einzelner Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).
2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von

einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z. B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 lit. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.
4. Der Begriff „Gesundheitsberuf“ ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

3. Orientierungshilfen und Muster

3.1
Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Stand: 19.02.2014 Version: 1.1

Inhaltsübersicht

1.
Chancen und Risiken einer Videoüberwachung

Videoüberwachung (zum Begriff s. 2.1.1) ist vermeintlich in der Lage, bei gewissen Sicherheitsproblemen eine einfache Lösung zu bieten. So können etwa unübersichtliche Gebäudekomplexe zu verschiedensten Tages- und Nachtzeiten leicht überwacht werden. Die Aufsicht über das System kann zentral und mit wenig Personalaufwand erfolgen. Die Technik ist erschwinglich und regelmäßig ohne besondere Kenntnisse zu installieren. Die datenschutzrechtliche Relevanz der Videoüberwachung wird von den Betreibern einer Videoüberwachungsanlage jedoch häufig falsch eingeschätzt. Jeder Mensch hat grundsätzlich das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mit Hilfe von Kameras beobachtet oder aufgezeichnet wird. Die Tatsache beobachtet zu werden, kann bei vielen Personen eine Änderung ihres Auftretens bewirken, weil die Gefahr besteht, dass das eigene Verhalten überprüft und nicht autorisiert z. B. im Internet veröffentlicht wird. Bei einer ununterbrochenen Überwachung kann das Wissen, dass jede Bewegung und jede Geste von einer Kamera überwacht wird, mit weitreichenden psychologischen Auswirkungen verbunden sein. Der Einzelne fühlt sich ständig beobachtet und ist dadurch einem permanenten Überwachungsdruck ausgesetzt. Mit dem Einsatz von Videoüberwachungsanlagen sind weitere Risiken verbunden. Es besteht die Gefahr, dass Aufzeichnungen missbraucht oder für fremde Zwecke genutzt werden. Elektronische Bilder können ohne Weiteres gespeichert, kopiert und unbegrenzt an eine Vielzahl von Empfängern in kürzester Zeit und ohne finanziellen Aufwand weitergeleitet werden. Umfassende räumliche und zeitliche Überwachungen ermöglichen die Erstellung von Bewegungs- und Verhaltensprofilen. Hinzu kommt, dass „intelligente“ Videoüberwachungssysteme keine reine Zukunftsmusik mehr sind. Technisch ist es beispielsweise möglich, gezielt einzelne Personen automatisiert über eine große räumliche Distanz zu verfolgen und mittels Bilderabgleich in Datenbanken eindeutig zu identifizieren. Machbar ist es auch, „auffällige“ oder vermeintlich nicht normale Bewegungen und Verhaltensmuster herauszufiltern, anzuzeigen und gegebenenfalls Alarm auszulösen.

Diese Orientierungshilfe soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Sofern mit einer Kamera personenbezogene Daten erhoben werden, also z. B. Personen oder Kfz-Kennzeichen erkennbar sind, bedarf es nach dem sog. Verbot mit Erlaubnisvorbehalt einer rechtlichen Grundlage für die Datenverarbeitung. Zu unterscheiden ist dabei zwischen der Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen (§ 6b des Bundesdatenschutzgesetzes [BDSG]),

der Videoüberwachung von Beschäftigten (§ 32 Abs. 1 BDSG) und einer sonstigen Videoüberwachung in nicht öffentlich zugänglichen Räumen (§ 28 BDSG). Am Ende finden Sie einen Fragenkatalog, der Verantwortlichen und Datenschutzbeauftragten als Checkliste dienen kann.

2.
Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen

Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welche die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Nicht-öffentliche Stellen sind private Betreiber von Videotechnik, z. B. Unternehmen oder Privatpersonen.

2.1
Anwendungsbereich und Voraussetzungen des § 6b Absatz 1 BDSG

Im Folgenden wird beschrieben, wann diese Vorschrift Anwendung findet und welche Anforderungen sie an eine Videoüberwachungsanlage stellt.

2.1.1
Wann liegt eine Videoüberwachung vor?

§ 6b Absatz 1 BDSG definiert die Videoüberwachung als Beobachtung mit „optisch-elektronischen Einrichtungen“. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Dabei ist irrelevant, ob sie über eine Zoomfunktion oder eine Schwenkvorrichtung verfügen, ob die Kamera stabil montiert oder frei beweglich ist. Auch der Einsatz von Webcams, Wildkameras, digitalen Fotoapparaten oder Mobiltelefonen mit integrierter Kamera ist grundsätzlich als Videoüberwachung anzusehen (s. hierzu auch Nr. 3.1). Voraussetzung ist dabei jeweils die Erhebung personenbezogener Daten, das heißt, dass Personen auf den Aufnahmen erkennbar sein müssen oder sonst Rückschlüsse auf die Identität einer Person möglich sind.

Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Eine Videoüberwachung liegt bereits vor, sobald die Möglichkeit der Beobachtung gegeben ist, das bedeutet, dass unabhängig von einer möglichen Speicherung oder Aufzeichnung der Bilder schon bei bloßer Live-Beobachtung mittels

optisch-elektronischer Einrichtung die Vorgaben des § 6b BDSG einzuhalten sind. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt. Damit unterfällt beispielsweise das Anfertigen von Fotos in kurzen Zeitintervallen ebenfalls der Vorschrift. Die gezielte Beobachtung einzelner Personen wird nicht vorausgesetzt. Die Überwachungsmaßnahme setzt selbst dann bereits mit der Inbetriebnahme der Kameras ein, wenn die Geräte erst im Bedarfs- oder Alarmfall aufzeichnen.

Bei bloßen Kameraattrappen oder unzutreffenden Hinweisen auf eine Videoüberwachung gehen die Datenschutzaufsichtsbehörden der meisten Bundesländer davon aus, dass das Bundesdatenschutzgesetz nicht zur Anwendung kommt, da es sich bei Attrappen um keine optisch-elektronische Einrichtungen handelt und deshalb keine personenbezogenen Daten erhoben werden. Allerdings erweckt auch das Anbringen von Kameraattrappen und unzutreffenden Hinweisen bei Personen, die diese zur Kenntnis nehmen, regelmäßig den Eindruck, dass sie tatsächlich videoüberwacht werden. Da die fehlende Funktionsfähigkeit der Kamera von außen nicht erkennbar ist, kann ein Überwachungsdruck hervorgerufen werden[1], der eine Beeinträchtigung des Persönlichkeitsrechts darstellen und damit zivilrechtliche Abwehransprüche auslösen kann. Diese müssen notfalls im Klageweg durchgesetzt werden. Ob darüber hinaus ein aufsichtsbehördliches Einschreiten gegen eine Attrappe in Betracht kommt, differiert danach, ob die örtlich zuständige Aufsichtsbehörde hierfür auch eine sachliche Zuständigkeit anerkennt. Dies erfahren Betroffene ggf. auf Nachfrage.

2.1.2
Was ist ein öffentlich zugänglicher Raum?

Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von Jedermann genutzt oder betreten werden dürfen. Ein öffentlicher Raum liegt auch dann vor, wenn für den Zugang besondere allgemeine Voraussetzungen, wie etwa ein bestimmtes Mindestalter, erfüllt sein müssen, ein Eintrittspreis zu errichten ist oder die Öffnung nur zu bestimmten Zeiten erfolgt. Darauf, ob der überwachte Bereich Privateigentum ist oder nicht, kommt es nicht an. Zu den öffentlich zugänglichen Räumen gehören neben öffentlichen Verkehrsflächen beispielsweise Ausstellungsräume eines Museums, Verkaufsräume, Schalterhallen, Tankstellen, Biergärten, öffentliche Parkhäuser, Gasträume von Gaststätten oder Hotelfoyers.

Nicht öffentlich zugänglich sind demgegenüber Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Hierzu gehören etwa Büros oder Produktionsbereiche ohne Publikumsverkehr. Entscheidend ist hierbei, dass die Nicht-Öffentlichkeit durch Verbotsschilder oder den Kontext der Umgebung erkennbar ist. Die eigene private Wohnung zählt z. B. zu den nicht öffentlich zugänglichen Räumen. Zu beachten ist allerdings, dass die Einordnung als nicht öffentlich zugänglicher Raum vom Einzelfall abhängig ist. Das Treppenhaus eines Wohnhauses ist beispielsweise grundsätzlich ein nicht öffentlich zugänglicher Raum. Befindet sich im Haus allerdings eine Arztpraxis oder eine Anwaltskanzlei mit offenem Publikumsverkehr, dann ist dies bereits ausreichend, um das Treppenhaus während der Geschäftszeiten als öffentlich zugänglich einzuordnen. Eine Videoüberwachung nicht öffentlich zugänglicher Räume kann unter Umständen nach § 28 BDSG zu beurteilen sein (siehe unten Nr. 5.). Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die sich dort befindlichen Personen erfasst werden. Bei einem Nachbargrundstück handelt es sich nicht um einen öffentlichen Raum; dessen Beobachtung ist daher nicht von § 6b BDSG erfasst. Allerdings greift eine Überwachung von Nachbargrundstücken in die Persönlichkeitsrechte des Nachbarn ein. Dieser kann sich daher auf zivilrechtlichem Weg mittels Abwehr- und Unterlassungsansprüchen gegen die Videoüberwachung zur Wehr setzen (zur Videoüberwachung im Nachbarschaftsverhältnis vgl. unten Nr. 5).

2.1.3
Zulässigkeit einer Videoüberwachung öffentlich zugänglicher Räume

Nach § 6b Absatz 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (2.1.3.1) erforderlich ist (2.1.3.2) und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen (2.1.3.3).

2.1.3.1
Zweck der Videoüberwachung

Bevor eine Videoüberwachung installiert wird, ist zu konkretisieren, welches Ziel damit erreicht werden soll. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder recht-

licher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren. Auch die Beweissicherung durch die Aufzeichnung kann ein solches berechtigtes Interesse darstellen.

In bestimmten Fällen kann auch eine abstrakte Gefährdungslage ausreichend sein, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die wertvolle Ware verkaufen (z. B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte potenziell besonders gefährdet sind (z. B. Tankstellen).

Darüber hinaus ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret anzugeben.

2.1.3.2
Geeignetheit und Erforderlichkeit der Videoüberwachung

Vor dem Einsatz eines Videoüberwachungssystems ist zu überprüfen, ob es tatsächlich für den festgelegten Zweck geeignet und erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden Mittel erreicht werden kann. Vor der Installation einer Videoüberwachungsanlage muss man sich deshalb mit zumutbaren alternativen Methoden auseinandersetzen, die in das Persönlichkeitsrecht des Einzelnen weniger eingreifen. Eine Umzäunung, regelmäßige Kontrollgänge von Bewachungspersonal, der Einsatz eines Pförtners, der Einbau von Sicherheitsschlössern oder von einbruchssicheren Fenstern und Türen können beispielsweise ebenfalls einen wirksamen Schutz gegen Einbruch und Diebstahl bieten. Das Auftragen von spezieller Oberflächenbeschichtung kann Schutz vor Beschädigungen durch Graffiti bieten.

Des Weiteren muss vor Inbetriebnahme einer Kameraanlage eine Überprüfung dahingehend erfolgen, an welchen Orten und zu welchen Zeiten eine Überwachung unbedingt notwendig erscheint. Häufig kann eine Überwachung in den Nachtstunden oder außerhalb der Geschäftszeiten ausreichend sein.

Im Rahmen der Erforderlichkeit ist ferner zu untersuchen, ob eine reine Beobachtung im Wege des Live-Monitorings ausreichend ist oder ob es zum Erreichen des Überwachungszwecks einer (regelmäßig eingriffsintensiveren) Aufzeichnung bedarf. In diesem Zusammenhang ist zu betonen, dass eine reine Aufzeichnung (blackbox) für präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. Sicherheitspersonal unmittelbar eingreifen kann. Das bedeutet, dass eine Videoaufzeichnung zur Verhinderung von Unfällen oder Straftaten nicht geeignet ist.

Unter dem Aspekt der Datenvermeidung und Datensparsamkeit ist weiterhin zu prüfen, ob durch den Einsatz spezieller Technik bestimmte Bereiche des Aufnahmefeldes ausgeblendet oder die Gesichter der sich in diesen Bereichen aufhaltenden Personen „verschleiert“ werden können.

2.1.3.3
Beachtung der schutzwürdigen Interessen der/des Betroffenen

Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Maßstab der Bewertung ist das informationelle Selbstbestimmungsrecht als besondere Ausprägung des Persönlichkeitsrechts auf der einen und der Schutz des Eigentums oder der körperlichen Unversehrtheit auf der anderen Seite. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist häufig die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art der erfassten Informationen (Informationsgehalt), Umfang der erfassten Informationen (Informationsdichte, zeitliches und räumliches Ausmaß), den betroffenen Personenkreis, die Interessenlage der betroffenen Personengruppen, das Vorhandensein von Ausweichmöglichkeiten sowie Art und Umfang der Verwertung der erhobenen Daten bestimmt. In den Fällen, in denen die Videoaufnahmen nicht nur auf einen Monitor übertragen, sondern auch aufgezeichnet werden sollen, ist eine diesbezügliche Abwägung mit den schutzwürdigen Interessen der Betroffenen erneut vorzunehmen.

Grundsätzlich unzulässig sind Beobachtungen, die die Intimsphäre der Menschen verletzen, etwa die Überwachung von Toiletten, Saunas, Duschen oder Umkleidekabinen. Die schutzwürdigen Interessen überwiegen außerdem häufig dort, wo die Entfaltung der Persönlichkeit im Vordergrund steht, beispielsweise in Restaurants, Erlebnis- und Erholungsparks, wo Leute

kommunizieren, essen und trinken oder sich erholen. Auch eine permanente Überwachung, der eine betroffene Person nicht ausweichen kann, stellt einen gravierenderen Eingriff dar als eine Beobachtung, die lediglich zeitweise erfolgt und nur Teilbereiche des Raumes erfasst. Dies ist zum Beispiel bei der dauerhaften Überwachung von öffentlichen Zufahrten und Eingängen zu Mehrfamilienhäusern relevant, da die Bewohner auf die Nutzung des überwachten Bereichs angewiesen sind. Grundsätzlich gilt, je mehr persönliche Informationen aufgrund der Überwachung erhoben werden, desto intensiver ist der Eingriff in die Grundrechte und in die schutzwürdigen Interessen der Betroffenen.

Ermöglicht die Qualität der Aufnahme keine Personenbeziehbarkeit, sind schutzwürdige Interessen Betroffener schon deshalb nicht verletzt, weil es an einer Datenerhebung im Sinne des § 3 Absatz 3 BDSG fehlt.

2.2
Einzelne Maßnahmen vor Einrichtung einer Videoüberwachung

Vor dem Einsatz einer Videoüberwachungsanlage gilt es einige Maßnahmen und Voraussetzungen nach dem Bundesdatenschutzgesetz durchzuführen und einzuhalten.

2.2.1
Verfahrensverzeichnis, Vorabkontrolle, Sicherungspflichten

Vor Beginn der Videoüberwachung ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme (vgl. Nr. 2.1.3.1) schriftlich festzulegen. Zudem sind technische und organisatorische Maßnahmen zu treffen (§ 9 BDSG), um die Sicherheit der Daten zu gewährleisten. Vor der Inbetriebnahme einer Videoüberwachung ist eine Vorabkontrolle nach § 4d Absatz 5 BDSG erforderlich, wenn bei dem Einsatz der Videotechnik von besonderen Risiken für die Rechte und Freiheiten der Betroffenen auszugehen ist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62).

Die/der betriebliche Datenschutzbeauftragte hat gemäß § 4d Absatz 6 BDSG die Vorabkontrolle durchzuführen und das Ergebnis sowie die Begründung schriftlich zu dokumentieren. Unabhängig von der Durchführung einer Vorabkontrolle ergibt sich das Erfordernis der vorherigen Zweckbestimmung aus § 6b Absatz 1 Nr. 3 BDSG, wenn die Videoüberwachung zur Wahrnehmung berechtigter Interessen erfolgt. Darüber hinaus ist für Verfahren, die automatisiert Daten verarbeiten, eine Verfahrensübersicht zu erstellen (vgl.

§ 4g Absatz 2 und 2a BDSG). Eine Videoüberwachung ist jedenfalls dann, wenn sie mittels digitaler Technik erfolgt, als automatisierte Verarbeitung zu qualifizieren. Welche Angaben in diese Übersicht aufgenommen werden müssen, zählt § 4e Satz 1 BDSG verbindlich und abschließend auf. Der dort geforderten allgemeinen Beschreibung der technisch-organisatorischen Maßnahmen zum Schutz der Daten kommt bei der Videoüberwachung besondere Bedeutung zu. Die Videobilddaten unterliegen wegen der sich aus einer unsachgemäßen Handhabung möglicherweise für den Betroffenen ergebenden Beeinträchtigungen entsprechend hohen Schutzkontrollen sowohl hinsichtlich des Zutritts, Zugangs und Zugriffs, aber auch der Weitergabe an Strafverfolgungsbehörden im Deliktfall. In der Verfahrensübersicht sind darüber hinaus die zugriffsberechtigten Personen zu benennen.

Die Verfahrensübersicht ist von der verantwortlichen Stelle zu erstellen und dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Dieser muss die Inhalte der Verfahrensübersicht bis auf die Angaben zu dem Bereich des Datensicherheitsmanagements auf Antrag jedermann zugänglich machen. Dieses öffentlich zugängliche Papier nennt man Verfahrens- oder auch „Jedermannverzeichnis“.

Sofern keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, fällt dem Leiter der nicht-öffentlichen Stelle die Pflicht zu, die Erfüllung dieser Aufgaben des betrieblichen Datenschutzbeauftragten in anderer Weise sicherzustellen.

2.2.2
Hinweispflicht

Nach § 6b Absatz 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mit Hilfe entsprechender Schilder oder graphischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

2.3
Durchführung einer zulässigen Videoüberwachung

2.3.1
Speicherdauer

Gemäß § 6b Absatz 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ist es beispielsweise an einer Tankstelle zu keinem Überfall oder Diebstahl gekommen, werden Videoaufzeichnungen für Beweiszwecke nicht mehr benötigt und sind daher zu löschen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können.[2]

Das bedeutet, dass Videoaufzeichnungen grundsätzlich nach 48 Stunden zu löschen sind. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, etwa wenn an Wochenenden und Feiertagen kein Geschäftsbetrieb erfolgt. Da sich die gesetzliche Speicherdauer am Aufzeichnungszweck orientiert, kann der Zeitpunkt der Löschpflicht je nach Einzelfall variieren. Dem Löschungsgebot wird am wirksamsten durch eine automatisierte periodische Löschung, z. B. durch Selbstüberschreiben zurückliegender Aufnahmen, entsprochen.

2.3.2
Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Absatz 4 BDSG). Zweck dieser Regelung ist es, Transparenz zu schaffen und der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Eine Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen. Die Notwendigkeit einer Benachrichtigung besteht erst bei einer tatsächlichen Zuordnung; allein die Möglichkeit dazu macht eine Benachrichtigung noch nicht erforderlich. Die Benachrichtigung hat bei der erstmaligen Zuordnung zu erfolgen.

2.3.3
Tonaufzeichnungen

Für solche Überwachungsmaßnahmen ist im Strafgesetzbuch (StGB) mit § 201 (Verletzung der Vertraulichkeit des Wortes) eine Regelung enthalten, die es unter Strafandrohung verbietet, das nicht öffentlich gesprochene Wort aufzuzeichnen oder abzuhören. Sofern also eine Videoüberwachungskamera über eine Audiofunktion verfügt, ist diese irreversibel zu deaktivieren.

2.3.4
Überprüfung der Rechtmäßigkeitsvoraussetzungen

Der Betreiber einer Videoüberwachungsanlage ist verpflichtet, die rechtlichen Voraussetzungen für den Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Geeignetheit und Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kamera in Betrieb war, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachung nicht weiter betrieben werden. Dies kann auch Teilbereiche einer Überwachung betreffen. Das Ergebnis der Überprüfung sollte schriftlich dokumentiert werden.

3.
Besondere Fallkonstellationen

3.1
Webcams

Webcams ermöglichen es, Live-Aufnahmen ins Internet einzustellen und damit einer unbestimmten Zahl von Personen weltweit zugänglich zu machen. Problematisch ist dabei, dass Persönlichkeitsrechtsverletzungen bei einer Live-Übertragung nicht mehr rückgängig gemacht werden können. Für zufällig von der Kamera erfasste Personen besteht daher ein großes Risiko, das durch die steigende Qualität und die einfache Möglichkeit der technischen Vervielfältigung und Bearbeitung der Aufnahmen noch erhöht wird. Der Einsatz einer Webcam ist nur dann datenschutzrechtlich unbedenklich, sofern auf den aufgenommenen Bildern – etwa aufgrund der Kamerapositionierung, fehlender Zoom-Möglichkeiten oder niedriger Auflösung – Personen oder Kfz-Kennzeichen nicht erkannt werden können.

3.2
Videoüberwachung in der Gastronomie

Die Videoüberwachung des Gastraumes einer Gaststätte[3] ist nach § 6b BDSG im Regelfall datenschutzrechtlich unzulässig. Jedenfalls die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind Kundenbereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und damit nicht mit Videokameras überwacht werden dürfen.[4]

Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts der Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechtigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann. Gleiches gilt für Café-und Gastrobereiche in Bäckereien, Tankstellen, Hotels etc.

4.
Videoüberwachung von Beschäftigten

Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden, zum Beispiel in Verkaufsräumen im Einzelhandel. In solchen Fällen ist nicht nur die Persönlichkeitssphäre der Kunden betroffen, sondern es kommt auch zu einer Überwachung der dort tätigen Beschäftigten. Für solche Bereiche, in denen die Wahrscheinlichkeit von Straftaten zu einem geschäftstypischen Risiko gehört und die Erfassung der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, überwiegt in Einzelfällen das berechtigte Interesse des Arbeitgebers, Straftaten vorzubeugen. Dennoch ist bei der Installation der Videoüberwachung das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich Beschäftigte länger aufhalten, erforderlich. Je weniger Rückzugsmöglichkeiten den Beschäftigten in nicht überwachten Bereichen zur Verfügung stehen, desto eher überwiegen deren schutzwürdige Interessen. Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten der Beschäftigten durch eine Videoanlage kann in der Regel nicht auf § 32 Absatz 1 Satz 1 BDSG gestützt werden. Denkbar sind offene Überwachungsmaßnahmen danach jedoch insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders

gefahrträchtigen Arbeitsbereichen erforderlich ist. Jedoch ist in diesem Zusammenhang der Erfassungsbereich auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte soweit wie möglich auszublenden. Eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen Dienstablauf zu gewährleisten, ist nicht gerechtfertigt.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nach § 32 Absatz 1 Satz 2 BDSG nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab 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.

Eine Videoüberwachung, die in nicht öffentlich zugänglichen Räumen stattfindet und nicht in Zusammenhang mit dem Beschäftigungsverhältnis steht, ist an den Voraussetzungen des § 28 Absatz 1 Satz 1 Nr. 2 BDSG zu messen. Der Einsatz von Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. So können ausnahmsweise auch Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Fokus der Überwachung steht und nicht permanent erfasst wird, z. B. der nächtliche Wachmann, der die zum Zweck der Verhinderung und Aufklärung von Diebstählen videoüberwachten Lagerräume kontrolliert, in denen wertvolle Ware aufbewahrt wird. Aber auch hier ist zuvor zu prüfen, ob weniger einschneidende Mittel in Betracht kommen.

Für die Bewertung der Zulässigkeit einer solchen Maßnahme ist ergänzend die Rechtsprechung des Bundesarbeitsgerichts[5] zugrunde zu legen.

In wenigen Ausnahmefällen kann danach die Überwachung von Beschäftigten mittels Kameras durch den Arbeitgeber dann zulässig sein, wenn sie offen erfolgt, die Beschäftigten also wissen, dass ihr Arbeitsplatz videoüberwacht wird. Entscheidend ist, ob der Arbeitgeber ein berechtigtes Interesse an den Kameraaufnahmen hat, etwa um Diebstählen oder Vandalismus durch sein Personal vorzubeugen. Hat er ein solches, berechtigt ihn dieses jedoch nicht ohne Weiteres zur Überwachung. Vielmehr muss sein Interesse mit den schutzwürdigen Interessen des Beschäftigten, nicht in seinem Persönlichkeitsrecht verletzt zu werden, abgewogen werden. Das Persönlichkeitsrecht schützt den Beschäftigten vor einer lückenlosen Überwachung am Arbeitsplatz durch Videoaufnahmen, die ihn einem ständigen Überwachungsdruck aussetzen, dem er sich nicht entziehen kann. Deswegen überwiegt das Beschäftigten-

interesse, von einer derartigen Dauerüberwachung verschont zu bleiben, wenn der Arbeitgeber mit der Überwachung nur befürchteten Verfehlungen seiner Beschäftigten präventiv begegnen will, ohne dass hierfür konkrete Anhaltspunkte bestehen. In der Abwägung wird auch gewichtet, ob den Beschäftigten überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich verbleibt. Zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz sind Kameras keinesfalls erlaubt. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind ebenfalls von der Überwachung auszunehmen. Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die Videoüberwachung praktisch die einzig verbleibende Möglichkeit zur Aufklärung oder zur Verhinderung des Missstandes darstellt und insbesondere im Hinblick auf den angerichteten oder zu verhindernden Schaden nicht unverhältnismäßig ist.

Kann die Datenerhebung und -verarbeitung im Beschäftigungsverhältnis nicht auf eine Rechtsgrundlage gestützt werden, ist die Videoüberwachung wegen § 4 Absatz 1 BDSG (Verbot mit Erlaubnisvorbehalt) unzulässig. Eine etwaige arbeitgeberseitig eingeholte Einwilligung des Beschäftigten ist irrelevant, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4a Absatz 1 Satz 1 BDSG mangelt.

Soweit die Videoüberwachung den gesetzlichen Vorgaben entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung näher geregelt werden. Die Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sollten näher beschrieben werden. Dazu gehören insbesondere:

– Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
– Zweckbindung
– Datenvermeidung- und Datensparsamkeit
– Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
– Empfänger der Daten
– Rechte der Betroffenen
– Löschfristen
– technische und organisatorische Maßnahmen wie beispielsweise das Berechtigungskonzept

Soweit ein Betriebsrat nicht existiert, sollte der Arbeitgeber entsprechende Dienstanweisungen erstellen.

Zulässige Verfahren zur Videoüberwachung ermöglichen in der Regel eine Bewertung der Persönlichkeit der betroffenen Beschäftigten einschließlich

ihrer Fähigkeiten, ihrer Leistungen und ihres Verhaltens. Daher ist nach § 4d Absatz 5 Satz 2 Nr. 2 BDSG regelmäßig eine Vorabkontrolle durchzuführen (vgl. oben Nr. 2.2.1).

5.
Sonstige Videoüberwachung durch nicht-öffentliche Stellen, insbesondere Videoüberwachung durch Nachbarn oder Vermieter

Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kameras zu unterscheiden. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den Grundstücksgrenzen endet. Wer außer seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass – quasi nebenbei – auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mitüberwacht werden.

Sofern sich die Videoüberwachung auf das Grundstück des Nachbarn erstreckt, ohne dass eine öffentlich zugängliche Fläche betroffen ist, ist die Anwendbarkeit des Bundesdatenschutzgesetzes zumeist deshalb zu verneinen, weil es sich um eine persönliche bzw. familiäre Tätigkeit im Sinne des § 1 Absatz 2 Nr. 3 BDSG handelt, die vom Regelungsbereich des Bundesdatenschutzgesetzes ausgenommen ist. Dies hat zur Folge, dass die Anlage nicht der Kontrolle der Datenschutzaufsichtsbehörden unterliegt. Videoüberwachten Nachbarn stehen jedoch unabhängig davon unter Umständen zivilrechtliche Unterlassungs- und Abwehransprüche zu. Diese müssten auf dem Zivilrechtsweg gegebenenfalls unter Einschaltung eines Rechtsanwalts geltend gemacht werden. Darüber hinaus kann das Beobachten fremder Grundstücke mit einer Videoanlage strafrechtliche Konsequenzen haben, wenn damit der höchst persönliche Lebensbereich der beobachteten Person verletzt wird (vgl. § 201a des Strafgesetzbuchs).

Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b BDSG richtet (vgl. oben Nr. 2.1.2). In

diesen Fällen greift § 28 BDSG, wonach ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. Außerdem besteht in diesen Fällen ebenfalls die Möglichkeit, mit zivilrechtlichen Unterlassungs- und Abwehransprüchen gegen einen etwaigen Eingriff in das Persönlichkeitsrecht vorzugehen. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum oder im Fahrstuhl selbst, einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. In der hierzu ergangenen zivilrechtlichen Rechtsprechung[6] besteht Einigkeit darüber, dass eine Rundumüberwachung des sozialen Lebens nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Schmierereien, Verschmutzungen oder einmaligen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

6.
Checkliste für den Betreiber einer Videoüberwachung öffentlich zugänglicher Räume

Planen Sie die Installation von Videokameras oder betreiben Sie bereits eine Videoüberwachungsanlage? Folgende Fragen sollten Sie für eine zulässige Überwachungsmaßnahme beantworten können:

1. Welche Bereiche sollen überwacht werden?
   - öffentlich zugänglicher Raum (z. B. Kundenbereiche),
   - Mitarbeiterräume,
   - öffentliche Flächen (z. B. Gehwege)
2. Dient die Videoüberwachung der
   - Wahrung des Hausrechts oder
   - Wahrung eines anderen berechtigten Interesses (Zweck)? Wenn ja, welchem?
   - Besteht eine Gefährdungslage und auf welche Tatsachen, z. B. Vorkommnisse in der Vergangenheit, gründet sich diese?
3. Wurde der Zweck der Videoüberwachung schriftlich festgelegt?
4. Warum ist die Videoüberwachung geeignet, den festgelegten Zweck zu erreichen?
5. Warum ist die Videoüberwachung erforderlich und warum gibt es keine milderen Mittel, die für das Persönlichkeitsrecht der Betroffenen weniger einschneidend sind?

6. Welche schutzwürdigen Interessen der Betroffenen haben Sie mit welchem Ergebnis in die Interessenabwägung einbezogen?
7. Ist eine Beobachtung der Bilder auf einem Monitor ohne Aufzeichnung der Bilddaten ausreichend?

   Wenn nein, warum nicht?
8. Sofern aufgezeichnet wird, wann werden die Aufnahmen gelöscht? Wenn das Löschen nicht innerhalb von 48 Stunden erfolgt, begründen Sie bitte das spätere Löschen.
9. Zu welchen Zeiten erfolgt die Videoüberwachung und wer hält sich üblicherweise zu dieser Zeit im überwachten Bereich auf?
10. Wenn eine Videoüberwachung rund um die Uhr erfolgt, warum halten Sie sie für erforderlich bzw. warum kann sie nicht zeitlich eingeschränkt werden, z. B. auf außerhalb der Geschäftszeiten oder die Nachtstunden?
11. Werden bestimmte Bereiche der Überwachung ausgeblendet oder verpixelt?

    Wenn nein, warum nicht?
12. Über welche Möglichkeiten verfügt die Videokamera und welche hiervon sind für die Überwachung nicht erforderlich und ggf. zu deaktivieren?
    - hinsichtlich der Ausrichtung, z. B. schwenkbar oder variabel, Dome-Kamera
    - bezüglich der Funktionalität, z. B. Zoomobjektive, Funkkameras, Audiofunktion
13. Wurde geprüft, ob eine Vorabkontrolle erforderlich ist und wurde sie ggf. durch die bzw. den betrieblichen Datenschutzbeauftragten durchgeführt? Wenn nein, warum ist eine Vorabkontrolle nicht erforderlich?
14. Wird auf die Videoüberwachung so hingewiesen, dass der Betroffene vor Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann?
15. Wird in dem Hinweis die verantwortliche Stelle genannt?
16. Unter welchen Voraussetzungen wird Einsicht in die Aufnahmen genommen?

    Durch wen?

    Ist die Protokollierung der Einsichtnahme sichergestellt?

    Wurden die zugriffsberechtigten Personen auf das Datengeheimnis verpflichtet?
17. Wurden die technisch-organisatorischen Maßnahmen zum Schutz der Daten nach § 9 BDSG (und der Anlage hierzu) getroffen?

18. Gibt es im Unternehmen einen Betriebsrat und wurde mit diesem eine Betriebsvereinbarung zur Videoüberwachung getroffen?

Rein vorsorglich weisen wir darauf hin, dass eine Beschäftigung mit diesen Fragen nicht automatisch zur Zulässigkeit der Videoüberwachungsmaßnahme führt.

Haben Sie zum Betrieb einer Videoüberwachungsanlage konkrete Fragen, können Sie sich gerne an die für Sie zuständige Datenschutzaufsichtsbehörde wenden. Maßgeblich ist grundsätzlich der Sitz des Betreibers. Eine Übersicht über die Kontaktdaten erhalten Sie beispielsweise unter http://www.baden-wuerttemberg.datenschutz.de/die-aufsichtsbehorden-der-lander/.

[1] LG Bonn, Urteil vom 16.11.2004-8 S 139/04; AG Lichtenberg, Beschluss vom 24.01.2008 – 10 C 156/07.

[2] Vgl. die Gesetzesbegründung, BT-Drs. 14/5793, S. 63.

[3] Gemeint ist die Gaststätte im Sinne des Gaststättengesetzes (GastG), d. h. ein Betrieb, in dem Getränke und/oder Speisen zum Verzehr an Ort und Stelle verabreicht werden und der jedermann oder bestimmten Personenkreisen zugänglich ist (vgl. § 1 GastG). Unter den Gaststättenbegriff fallen somit auch Cafés, Imbisslokale, Schnellrestaurants etc.

[4] Vgl. AG Hamburg, Urteil vom 22.04.2008 – 4 C 134/08.

[5] Vgl. insb. BAG, Urteil vom 27.03.2003 – 2 AZR 51/02; Beschluss vom 29.06.2004 – 1 ABR 21/03; Beschluss vom 14.12.2004 – 1 ABR 34/03; Beschluss vom 26.08.2008 – 1 ABR 16/07; Urteil vom 21.06.2012 – 2 AZR 153/11.

[6] Vgl. beispielsweise LG Berlin, Urteil vom 23.05.2005 – 62 S 37/05; KG Berlin, Beschluss vom 04.08.2008 – 8 U 83/08; AG München, Urteil vom 16.10.2009 – 423 C 34037/08

3.2
Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)

Inhaltsübersicht

1. Datenschutz-Grundverordnung (DS-GVO) und Direktwerbung

1.1 Begriff der Werbung im Sinne der DS-GVO

Werbung bzw. Direktwerbung im Sinne der DS-GVO ist zum einen die von Unternehmen, Selbstständigen, Verbänden und Vereinen usw. durchgeführte Wirtschaftswerbung zum Aufbau und zur Förderung eines Geschäftsbetriebs. „Werbung“ wird hierzu in Art. 2 lit. a der EU-Richtlinie 2006/114/EG über irreführende und vergleichende Werbung vom 12.12.2006 definiert als „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern“.

Diese weitgreifende Betrachtungsweise von Werbung legen auch die Gerichte in ihren Entscheidungen zugrunde und sehen z. B. damit auch Zufriedenheitsnachfragen bei Kunden nach einem Geschäftsabschluss, Geburtstags- und Weihnachtsmailings usw. als Werbung an.

Zum anderen ist Werbung bzw. Direktwerbung im Sinne der DS-GVO, aber auch die Kontaktaufnahme durch Parteien, Verbände und Vereine oder karitative und soziale Organisationen mit betroffenen Personen, um ihre Ziele bekannt zu machen oder zu fördern (siehe zur Werbung von politischen Parteien z. B. BVerfG-Beschluss vom 01.08.2002, 2 BvR 2135/01).

1.2 Keine Detailregelungen dazu in der DS-GVO

Mit der DS-GVO sind alle detaillierten Regelungen des bisherigen Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung weggefallen (siehe bisher insbesondere § 28 Abs. 3 und 4 sowie § 29 BDSG-alt).

Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist in der DS-GVO, abgesehen von einer Einwilligung der betroffenen Person, eine Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein, sofern nicht die Interessen der betroffenen Person überwiegen. Anhaltspunkte für die zu treffende Abwägungsentscheidung enthält Erwägungsgrund (ErwGr.) 47 DS-GVO, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

1.3
Interessenabwägung

Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen bzw. Dritten als auch der betroffenen Person. Ein bloßes Abstellen auf abstrakte oder auf vergleichbare Fälle ohne Betrachtung des Einzelfalls genügt den Anforderungen der DS-GVO nicht.

Insoweit ergibt sich für die Interessenabwägung u. a. aus ErwGr. 47, dass die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen sind. Damit ist auch auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen.

Neben diesen ist aber auch zu fragen, was objektiv vernünftigerweise erwarten werden kann und darf. Entscheidend ist daher auch, ob die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.

Die Erwartungen der betroffenen Person werden bei Maßnahmen zur Direktwerbung auch durch die Informationen nach Art. 13 und 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt. Informiert der Verantwortliche transparent und umfassend über eine vorgesehene Verarbeitung von Daten für Zwecke der Direktwerbung, geht die Erwartung der betroffenen Personen in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden. Allerdings kann durch Transparenz der gesetzliche Abwägungstatbestand nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO nicht beliebig erweitert werden, da die Erwartungen an dem objektiven Maßstab der Vernunft gemessen werden müssen.

Die Datenverarbeitung muss ferner insgesamt im Hinblick auf die berechtigten Interessen erforderlich sein.

Zudem sind bei der Interessenabwägung die ohnehin geltenden allgemeinen Grundsätze aus Art. 5 Abs. 1 DS-GVO zu berücksichtigen, also insbesondere:

– faire Verfahrensweise
– dem Verarbeitungszweck angemessen
– in einer für die betroffene Person nachvollziehbaren Weise (insbesondere Nennung der Quelle der Daten, wenn Fremddaten verarbeitet werde)

1.3.1
Praxisfälle Interessenabwägung

Vorbehaltlich der konkreten Abwägung im Einzelfall und den ergänzenden Ausführungen zu Punkt 1.4 und 1.5 können folgende Grobkategorien für die Abwägung in der Praxis relevant werden:

Schutzwürdige Interessen dürften in der Regel nicht überwiegen, wenn im Nachgang zu einer Bestellung allen Kunden (ohne Selektion) postalisch ein Werbekatalog oder ein Werbeschreiben zum Kauf weiterer Produkte des Verantwortlichen zugesendet wird.

Sofern es anhand eines Selektionskriteriums zu einer Einteilung in Werbegruppen kommt und sich kein zusätzlicher Erkenntnisgewinn aus der Selektion ergibt, wird die Interessenabwägung in der Regel ebenfalls zugunsten des Verantwortlichen ausfallen.

Eingriffsintensivere Maßnahmen wie automatisierte Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen, sprechen hingegen dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt. In diesen Fällen handelt es sich um Profiling, das nicht mehr auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden kann und damit die Einholung einer Einwilligung vor der Datenverarbeitung erforderlich macht. Das Widerspruchsrecht des Art. 21 DS-GVO reicht dann nicht aus.

Auch die Erstellung eines Profils unter Verwendung externer Datenquellen (z. B. Informationen aus sozialen Netzwerken) für Zwecke der Direktwerbung (Werbescores) wird in der Regel zu einem Überwiegen der schutzwürdigen Interessen der betroffenen Person führen.

Hinsichtlich der Übermittlung von Daten für Werbezwecke an Dritte sowie der Nutzung von Fremdadressen ist zu prüfen, ob dem Interesse der betroffenen Person ein höherer Stellenwert einzuräumen ist als dem Interesse des Verantwortlichen an der Übermittlung sowie des Dritten zur Nutzung von Fremdadressen zur Werbung. Insoweit erläutert ErwGr. 47, dass die Erwartungshaltung des Betroffenen auch davon bestimmt wird, ob eine maßgebliche

und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn diese Kunde des Verantwortlichen ist. Die Vorgaben des Art. 6 Abs. 4 DS-GVO sind ggf. zu beachten (Punkt 1.5).

1.4
Spezifische Regelungen für verschiedene Kontaktwege

Zu den konkreten Formen der Direktwerbung, also dem Kontaktweg zu den betroffenen Personen (Ansprache per Telefonanruf, E-Mail, Fax etc.), regelt das Wettbewerbsrecht, § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG), in welchen Fällen von einer unzumutbaren Belästigung der Beworbenen auszugehen und eine Werbung dieser Art unzulässig ist.

Weil Art. 6 Abs. 1 Satz 1 lit. f DS-GVO eine Verarbeitung personenbezogener Daten nur für zulässig erklärt, soweit die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, sind auch bei der datenschutzrechtlichen Beurteilung einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung die Wertungen in den Schutzvorschriften des UWG für die jeweilige Werbeform mit zu berücksichtigen. Wenn für den werbenden Verantwortlichen ein bestimmter Kontaktweg zu einer betroffenen Person danach nicht erlaubt ist, kann die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO auch nicht zugunsten der Zulässigkeit einer Verarbeitung dieser Kontaktdaten für Zwecke der Direktwerbung ausfallen.

1.4.1
Nutzen der E-Mail-Adressen von Bestandskunden

E-Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung (Bestandskunden) erhoben wurden, können grundsätzlich für E-Mail-Werbung genutzt werden, wenn dieser Zweck der E-Mail-Werbung entsprechend Art. 13 Abs. 1 lit. c DS-GVO den betroffenen Personen bei der Datenerhebung transparent dargelegt worden ist. Überwiegende schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO sind insbesondere dann nicht gegeben, wenn die in § 7 Abs. 3 UWG enthaltenen Vorgaben für elektronische Werbung eingehalten werden.

1.4.2
Nutzen von Telefonnummern

Für Anrufe bei Verbrauchern zu Zwecken der Direktwerbung sieht das UWG (§ 7 Abs. 2 Nr. 2) keine Ausnahme vom Einwilligungserfordernis vor, sodass ein

solches Nutzen von Telefonnummern ohne vorherige Einwilligung wegen der besonderen Auswirkungen dieser Werbeform (stärkere Belästigung/Störung) datenschutzrechtlich an den überwiegenden schutzwürdigen Interessen der betroffenen Personen gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO scheitert.

Bei Werbung mit einem Telefonanruf gegenüber einem **sonstigen Marktteilnehmer** (B2B) kommt es für die Zulässigkeit gemäß § 7 Abs. 2 Nr. 2 UWG darauf an, dass von dessen zumindest mutmaßlicher Einwilligung ausgegangen werden kann. Im B2B-Bereich stehen deshalb bei einem Nutzen von Telefonnummern für Werbeanrufe datenschutzrechtlich nicht von vornherein überwiegende schutzwürdige Interessen der telefonisch anzusprechenden Gewerbetreibenden nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO entgegen.

Siehe zum Verbot der Telefonwerbung gegenüber Gewerbetreibenden dazu ergänzend auch BGH, Urteil vom 16.11.2006, Az. I ZR 191/03, und BGH, Urteil vom 20.09.2007, Az. I ZR 88/05.

1.5
Zweckänderung

Sofern personenbezogene Daten für Werbezwecke verwendet werden sollen, die ursprünglich nicht (auch) zu Zwecken der Werbung erhoben worden sind, sind die Regelungen des Art. 6 Abs. 4 DSGVO (Zweckänderung) zu beachten. Eine Zweckänderung kann auch bei Fällen der Übermittlung an Dritte für Werbezwecke und bei der Nutzung von Fremdadressen für Werbung einschlägig sein, wenn sich die Datenverarbeitung nicht im Rahmen des Erhebungszweckes bewegt.

Um herauszufinden, ob der Werbezweck mit der ursprünglichen Zweckbestimmung vereinbar ist, müssen Verantwortliche eine sog. Kompatibilitätsprüfung durchführen.

2.
Informationspflichten[1]

2.1
Unterrichtung bei der Datenerhebung

Werden personenbezogene Daten unmittelbar bei der betroffenen Person erhoben, z. B. für Kauf- und Dienstleistungsverträge, Prospektanforderungen oder Gewinnspiele, ist diese umfassend nach Art. 13 Abs. 1 und 2 DS-GVO u. a. über die Zwecke der Verarbeitung der Daten zu unterrichten. Eine schon geplante oder in Betracht kommende Verarbeitung oder Nutzung der Daten

für Zwecke der Direktwerbung ist daher der betroffenen Person von Anfang an transparent darzulegen.

Bei einer nachträglichen Änderung der Verarbeitung auch für Zwecke der Direktwerbung schreibt Art. 13 Abs. 3 DS-GVO eine vorherige Information vor. Diese Information ist mit einem Hinweis auf das Werbewiderspruchsrecht zu versehen.

Grundsätzlich ist vom Verantwortlichen zum Zeitpunkt der Datenerhebung über alle Themen nach Art. 13 Abs. 1 und 2 DS-GVO zu informieren. Allerdings besteht schon rein praktisch nicht immer die Möglichkeit, der betroffenen Person alle Informationen aus Art. 13 Abs. 1 und 2 DS-GVO sofort vollständig geben zu können, z. B. bei Bestell-Postkarten als Zeitschriften-Beilage, bei Bestellungen am Telefon oder bei Kaufverträgen an Automaten. Die Aufsichtsbehörden unterstützen daher den Vorschlag der Artikel 29-Gruppe (WP 260, S. 17) für ein zweistufiges Informationsmodell.

Aus den Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO ergeben sich in der Regel folgende grundsätzliche Mindestanforderungen (entscheidend ist aber stets der Informationsbedarf im Einzelfall), die regelmäßig auf einer ersten Stufe umgesetzt werden müssen:

– Identität des für die Verarbeitung Verantwortlichen (Name einschließlich Kontaktdaten)
– Kontaktdaten des betrieblichen Datenschutzbeauftragten (soweit benannt)
– Verarbeitungszwecke und Rechtsgrundlage in Schlagworten
– Angabe des berechtigten Interesses, soweit die Verarbeitung darauf beruht
– Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
– Übermittlung in Drittstaaten
– Widerspruchsrecht nach Art. 21 DS-GVO
– Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Art. 13 Abs. 1 und 2 DS-GVO (wie Auskunftsrecht, Beschwerderecht), z. B. auch mittels QR-Code oder Internet-Link

2.2
Zeitpunkt der Information nach Art. 14 DS-GVO

Sollen personenbezogene Daten der betroffenen Person für Zwecke der Direktwerbung verarbeitet werden, die nicht von dieser Person selbst erhoben wurden, sind die Informationspflichten nach Art. 14 Abs. 1 und 2 DS-GVO zu beachten.

Eine unverzügliche oder separate Information fordert das Gesetz zwar nicht. Die Information muss jedoch innerhalb einer angemessenen Frist, jedenfalls zum Zeitpunkt der Aussendung einer Werbung, spätestens aber innerhalb eines Monats nach einer Verarbeitung erfolgen. Erfolgt die Information in Verbindung mit der ersten Werbezusendung, sind beide Bestandteile (Information und Werbetext) klar voneinander zu trennen und die Information (einschließlich Hinweis auf das Werbewiderspruchsrecht) entsprechend deutlich herauszustellen.

2.3
Information des Bestandes („Altfälle“)

Art. 13 und 14 DS-GVO stellen für die Informationspflichten vom Wortlaut her gesehen zunächst auf Datenerhebungen nach Wirksamwerden der DS-GVO ab („Werden personenbezogene Daten ... erhoben ...“).

Die Art. 29-Gruppe geht jedoch im Hinblick auf ErwGr. 171 Satz 2 („Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden.“) und der Grundsätze aus Art. 5 Abs. 1 lit. a DS-GVO zur Transparenz bei der Erarbeitung des WP 260 davon aus, dass bei den künftigen Kontakten mit den betroffenen Personen die neuen Informationspflichten in angemessener Weise umzusetzen bzw. nachzureichen sind (siehe dazu unter Nr. 2.1, Mindestinformationen, Verweis, wo alle Informationen unschwer zu erlangen sind).

3.
Einwilligung in die Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung

3.1
Gestaltung der Einwilligung

Die Einwilligung ist als eine Rechtmäßigkeitsvoraussetzung für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Satz 1 lit. a DS-GVO nur wirksam, wenn sie freiwillig und – bezogen auf einen bestimmten Fall – informiert abgegeben wird. Informiert setzt voraus, dass auch die Art der beabsichtigten Werbung (Brief, E-Mail/SMS, Telefon, Fax), die Produkte oder Dienstleistungen, für die geworben werden soll, und die werbenden Unternehmen genannt werden, um den Transparenzanforderungen von Art. 12 Abs. 1 und Art. 13 Abs. 1 lit. c DS-GVO sowie der bisher insoweit ergangenen Rechtsprechung zu genügen (siehe z. B. BGH-Urteil vom 14.03.2017, Az. VI ZR 721/15).

Erforderlich ist nach Art. 4 Nr. 11 und Art. 7 Abs. 2 DS-GVO eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung in einer klaren und einfachen Sprache oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person ihr Einverständnis zur Verarbeitung der sie betreffenden Daten erteilt.

Die Schriftform für datenschutzrechtliche Einwilligungen sieht die DS-GVO nicht als Regelfall vor. Verantwortliche haben allerdings gemäß Art. 5 Abs. 2 DS-GVO die Einhaltung der Rechtmäßigkeitsvoraussetzungen der Datenverarbeitung und gemäß Art. 7 Abs. 1 DS-GVO auch speziell das Vorliegen einer Einwilligung nachzuweisen. Um dieser Verpflichtung nachkommen zu können, ist den Verantwortlichen anzuraten, sich regelmäßig um eine Einwilligung in Schriftform mit handschriftlicher Unterschrift oder mindestens in Textform (z. B. E-Mail) zu bemühen.

Für Einwilligungen ist regelmäßig ein gesonderter Text oder Textabschnitt ohne anderen Inhalt zu verwenden. Soll sie zusammen mit anderen Erklärungen (insbesondere vertraglichen Erklärungen) schriftlich oder in einem elektronischen Format erteilt werden, so ist die datenschutzrechtliche Einwilligungserklärung gemäß Art. 7 Abs. 2 Satz 1 DS-GVO in einer von anderen Sachverhalten klar unterscheidbaren Weise darzustellen.

3.2
Einwilligung mit Übergabe von Visitenkarten

Visitenkarten, die von den betroffenen Personen auf Messen oder sonstigen Veranstaltungen ausdrücklich zur Informationszusendung oder weiteren geschäftlichen Kontaktaufnahme hinterlassen werden, können grundsätzlich eine wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO darstellen, wenn infolge weiterer Umstände für den Verantwortlichen eine Nachweisbarkeit der Einwilligung gegeben ist.

3.3
Double-Opt-In-Verfahren für elektronische Einwilligungen

Für das elektronische Erklären einer Einwilligung ist – zur Verifizierung der Willenserklärung der betroffenen Person – das Double-Opt-In-Verfahren geboten (je nach konkreter Art des Kontaktes: E-Mail oder SMS), wobei die Nachweis-Anforderungen des Art. 5 Abs. 2 DS-GVO und des BGH (Urteil vom 10.02.2011, I ZR 164/09) bei der Protokollierung zu berücksichtigen sind. Das bloße Abspeichern der IP-Adressen von Anschlussinhabern und die Behauptung, dass von diesen eine Einwilligung vorliege, genügen dem

BGH nicht. Der Nachweis der Einwilligung erfordert mehr, z. B. die Protokollierung des gesamten Opt-In-Verfahrens und des Inhalts der Einwilligung.

Ein solcher Nachweis reicht jedoch nicht im Fall der vorgesehenen Nutzung von über Website-Eintragungen erlangten Telefonnummern für Werbeanrufe aus. Mit der Übersendung einer Bestätigungs-E-Mail kann nämlich der Nachweis der Identität zwischen dem die Einwilligung mittels E-Mail Erklärenden und dem Anschlussinhaber der Telefonnummer nicht geführt werden. Eine schriftliche Einwilligung in die Nutzung einer E-Mail-Adresse und/oder einer Telefonnummer zu Werbezwecken ist regelmäßig die beste Möglichkeit für eine spätere Belegbarkeit einer Einwilligung.

3.4
„Koppelungsverbot“, Art. 7 Abs. 4 DS-GVO

Das bisher schon bestehende Koppelungsverbot für Werbung findet sich auch in der DS-GVO wieder, ist aber nicht mehr davon abhängig, ob ein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO).

3.5
„Verfall“ der Einwilligung, Verwirkung

Die Zivilgerichte sehen bei erteilten Einwilligungen zur werblichen Kontaktaufnahme teilweise keine unbegrenzte Gültigkeit. So hat das LG München I mit Urteil vom 08.04.2010, Az. 17 HK O 138/10, entschieden, dass eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert“ und deshalb insoweit keine rechtliche Grundlage mehr ist.

3.6
Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Art. 9 DS-GVO enthält keine Erlaubnisnorm für die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke der Werbung. Dies ist nur bei Vorliegen einer ausdrücklichen Einwilligung der betroffenen Person

zulässig. Von Relevanz ist dies z. B. für Unternehmen und Berufe des Gesundheitswesens (Apotheken, Sanitätshäuser, Optiker, Orthopäden usw.).

4.
Spezielle Sachverhalte bei der Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung

4.1
Veröffentlichung von Kontaktdaten in Rufnummernverzeichnissen

Telekommunikationsdienste-Anbieter müssen für die Zulässigkeit der Veröffentlichung von Telefonnummern und weiteren Kontaktdaten von Anschlussinhabern berücksichtigen, was die betroffene Person bei Vertragsabschluss oder später beantragt (keinerlei Veröffentlichung, Veröffentlichung nur in gedruckten oder auch in elektronischen Verzeichnissen). Andere Verzeichnisanbieter müssen dies bei der Interessenabwägung von nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu beurteilenden Sachverhalten beachten.

Eine darüber hinausgehende Verarbeitung solcher Kontaktdaten in Rufnummernverzeichnissen wäre unzulässig.

4.2
Datenerhebung anlässlich von Preisausschreiben, Katalog-/ Prospektanforderungen

Eine Verarbeitung von Postadressdaten für Zwecke der eigenen Direktwerbung aus der Durchführung von Preisausschreiben und Gewinnspielen sowie aufgrund von Katalog-und Prospektanforderungen ist nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig, wenn über die werbliche Datenverarbeitung informiert wurde; eine Einwilligung der betroffenen Personen ist bei solchen Sachverhalten dann nicht erforderlich. Die Anforderungen aus Nr. 2.1 sind zu beachten.

4.3
Keine Verwendung der Daten aus dem Impressum

Nicht zulässig ist hingegen das Auslesen der Daten aus einem Online-Impressum zum Zweck der werblichen Nutzung. Zwar sind diese Daten allgemein zugänglich, sie werden jedoch nicht freiwillig, sondern aufgrund der gesetzlichen Verpflichtung zur Anbieterkennzeichnung gem. § 5 TMG bzw. § 55 Abs. 2 RStV veröffentlicht. Mangels Freiwilligkeit der Veröffentlichung führt die Interessenabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO regelmäßig dazu, dass die werbliche Nutzung so erhobener Daten unzulässig ist. Zur

Vermeidung einer werblichen Ansprache mit diesen Daten kann ein Anbieter einer Internetseite vorsorglich einen Werbewiderspruch in sein Impressum aufnehmen.

4.4
Nennung des für die Verarbeitung der Daten Verantwortlichen sowie der Quelle von personenbezogenen Daten bei Fremdadressenbewerbung

Unter der Voraussetzung der Zulässigkeit der Datenübermittlung an Dritte (Punkt 1.3 bzw. Punkt 1.5) müssen der für die personenbezogenen Daten Verantwortliche, das werbende Unternehmen und die Quelle der Daten aus einer Werbung eindeutig hervorgehen und klar ersichtlich sein. Ein Verantwortlicher ist als konkrete juristische Person bzw. Firma mit ladungsfähiger Anschrift einschließlich E-Mail-Adresse zu nennen. Kurzbezeichnungen (wie XY-Group) oder Postfachanschriften genügen den Transparenzanforderungen von Art. 12 Abs. 1 Satz 1, Art. 13 Abs. 1 lit. a und Art. 14 Abs. 1 lit. a DS-GVO nicht.

4.5
Vertragliche Informationen, die gleichzeitig auch werbliche Informationen enthalten („Bei-pack-Werbung“)

Wenn Vertragspartnern vertragliche Informationen und damit verbunden auch eigene oder fremde werbliche Informationen per Brief zugesandt werden, ist dies in den Grenzen von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO möglich, solange von der betroffenen Person kein Werbewiderspruch nach Art. 21 Abs. 2 DS-GVO vorliegt.

Bei E-Mail-Werbung sind die Wertungen von § 7 Abs. 3 UWG zu beachten, wonach für Fremdwerbung keine Erleichterungen gelten.

4.6
Direktwerbung anhand von Dritten erlangten Postadressdaten („Freundschaftswerbung“)

Einer Praxis, weitere Postadressdaten bei Kunden- und Interessentenbesuchen durch Befragen Dritter zu erheben und für Zwecke der Direktwerbung zu verarbeiten, stehen regelmäßig die Grundsätze einer fairen und transparenten Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 lit. a und Art. 12 Abs. 1 DS-GVO entgegen.

4.7
Empfehlungswerbung

Der BGH sieht in einem Urteil vom 12.09.2013, I ZR 208/12 unverlangt versandte Empfehlungs-E-Mails als unzulässige Werbe-E-Mails an (ein Unternehmen hatte auf seiner Website die Möglichkeit für Nutzer eingerichtet, die E-Mail-Adresse eines Freundes anzugeben, um diesem dann unverlangt eine sog. Empfehlungs-E-Mail schicken zu können). Es komme für die Einordnung als Werbung nicht darauf an, dass das Versenden der Empfehlungs-E-Mails eines Unternehmens letztlich auf dem Willen eines Dritten beruhe.

Der BGH hat mit Urteil vom 14.01.2016, Az. I ZR 65/14, die Versendung von durch Facebook generierten E-Mails im Zusammenhang mit der Anmeldeprozedur „Freunde finden" als unzumutbar belästigende und damit unerlaubte Werbung eingestuft, weil diese E-Mails ohne vorherige ausdrückliche Einwilligung des Adressaten versandt werden.

Damit wird von den Gerichten klargestellt, dass über solche Konstrukte der Empfehlungswerbung das geltende Einwilligungserfordernis in E-Mail-Werbung nach § 7 Abs. 2 Nr. 3 UWG außerhalb von Bestandskundenverhältnissen im Sinne des § 7 Abs. 3 UWG nicht umgangen werden kann.

4.8
Mögliche Nutzungsdauer von Kontaktdaten der betroffenen Person für Zwecke der Direktwerbung

Nicht eindeutig zu beantworten ist die Frage, wie lange Kontaktdaten nach dem letzten aktiven Geschäfts- oder Direktwerbekontakt zu einer betroffenen Person für die werblichen Zwecke der Reaktivierung, Rückgewinnung etc. noch genutzt werden dürfen, bzw. ab wann nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO überwiegende schutzwürdige Interessen der betroffenen Person einer länger währenden werblichen Nutzung entgegenstehen.

Eine konkrete Frist hat der Gesetzgeber nicht vorgesehen.

Entscheidend ist, ob aufgrund der Art der Geschäftsbeziehung noch eine Erforderlichkeit zur weiteren Nutzung der Daten für Zwecke der Direktwerbung von dem Verantwortlichen nachvollziehbar dargelegt werden kann. Wenn nach der Rechtsprechung eine vor 17 Monaten erteilte und bisher nicht genutzte Einwilligung zur E-Mail-Werbung „ihre Aktualität verliert" und deshalb insoweit keine rechtliche Grundlage mehr ist (siehe hierzu unter 3.5), kann dieser zeitliche Maßstab auch bei der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu den vernünftigen Erwartungen der betroffenen Person eine Orientierung bieten, wenn nach einer langen „Werbepause" die Kontaktdaten der Person plötzlich wieder für eine Werbezusendung verarbeitet

werden. Auch dürfen keine überwiegenden schutzwürdigen Interessen der betroffenen Personen einer werblichen Nutzung entgegenstehen. So kann z. B. die Konditionenabfrage bei einem Bestattungsunternehmen keine längerfristige Datennutzung für werbliche Zwecke rechtfertigen.

5.
Hinweise zu Art. 21 Abs. 2 bis 4 DS-GVO

5.1
Werbewiderspruch und Wunsch nach Datenlöschung

Für die Umsetzung der Betroffenenrechte ist im Zweifelsfall von der betroffenen Person klarzustellen bzw. bei ihr zu klären, was sie mit ihrer Willenserklärung bewirken möchte. Möchte sie vorrangig von einer werblichen Ansprache durch das Unternehmen verschont bleiben, ist dafür die Aufnahme ihrer Kontaktdaten in eine Werbesperrdatei bei diesem Unternehmen das richtige Mittel zur Berücksichtigung ihres Willens. Bei der Nutzung von Fremddaten kann dann durch Abgleich mit der Werbesperrdatei sichergestellt werden, dass die Kontaktdaten dieser betroffenen Person nicht verwendet werden.

Solche Werbesperrdateien sind damit aufgrund von Art. 21 Abs. 3, Art. 17 Abs. 3 lit. b und Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zur Berücksichtigung der Werbewidersprüche von betroffenen Personen zulässig (zur notwendigen Sicherstellung der Beachtung des geltend gemachten Rechtsanspruchs).

Die betroffenen Personen müssen im Zusammenhang mit der Unterrichtung (Art. 12 Abs. 3 DS-GVO) über die Beachtung ihres Werbewiderspruchs auch über den Sinn und Zweck der Aufnahme ihrer Daten in eine Sperrdatei unterrichtet werden.

Wünscht eine betroffene Person ausdrücklich und allein eine Löschung aller Daten, sollte sie darauf hingewiesen werden, dass sie bei einem künftigen – rechtlich zulässigen – Einsatz von Fremddaten eventuell wieder Werbung erhalten kann.

Der Werbewiderspruch einer betroffenen Person kann sich, je nach ihrer Willenserklärung, datenschutzrechtlich gegen den Dateneignerin und/oder den Werbenden als Verantwortliche nach Art. 4 Nr. 7 DS-GVO richten. Beide müssen ggf. diesen Werbewiderspruch künftig berücksichtigen (durch Aufnahme in eine Werbesperrdatei). Im Hinblick auf Art. 12 Abs. 2 Satz 1 DS-GVO haben die Verantwortlichen für die effektive Durchsetzung des Widerspruchsrechts der betroffenen Person zusammenzuwirken (z. B. Weiterleitung des Widerspruchs).

Ergänzend kann ein Hinweis für die betroffene Person auf die sog. Robinsonlisten der Werbewirtschaft hilfreich sein, siehe z. B. unter www.ichhabediewahl.de oder www.robinsonliste.de.

5.2
Unterrichtung über das Werbewiderspruchsrecht

Art. 21 Abs. 4 DS-GVO verlangt, dass die betroffene Person in verständlicher und von anderen Informationen getrennter Form auf ihr Widerspruchsrecht gegen eine Verarbeitung ihrer personenbezogenen Daten für Zwecke der Direktwerbung einschließlich einem eventuellen damit in Verbindung stehenden Profiling hingewiesen werden muss. Aus Gründen der Nachweisbarkeit empfiehlt es sich, den Hinweis auf das Widerspruchsrecht bei jeder Werbesendung anzubringen.

Es ist nur dann von einer wirksamen Information im Sinne des Gesetzes auszugehen, wenn eine betroffene Person beim üblichen Umgang mit der Werbung oder mit Vertragsinformationen von dem Hinweis auf das Widerspruchsrecht Kenntnis erlangt. Das „Verstecken" der Information in langen AGB oder in umfangreichen Werbematerialien stellt keinen Hinweis im Sinne von Art. 21 Abs. 4 DS-GVO dar.

Im Sinne des Art. 12 Abs. 2 Satz 1 DS-GVO ist für die Einlegung des Werbewiderspruchs auch eine elektronische Kommunikationsmöglichkeit anzubieten.

5.3
Umsetzungsfrist des Werbewiderspruchs nach Art. 21 Abs. 3 DS-GVO

Die Umsetzung des Widerspruchs gegen die künftige Verarbeitung der Kontaktdaten einer betroffenen Person für Zwecke der Direktwerbung einschließlich einem eventuell damit in Verbindung stehenden Profiling muss in dem betreffenden Unternehmen unverzüglich erfolgen.

Wenn konkrete Werbeaktionen angelaufen sind und sich die Kontaktdaten der betroffenen Person schon in der technischen Verarbeitung befinden, kann es im Einzelfall für das Unternehmen unzumutbar sein, einen zwischenzeitlich eingegangenen Werbewiderspruch noch mit erheblichem Aufwand umzusetzen, z. B. einen bestimmten bereits adressierten Brief aus einer großen Menge herauszusortieren.

Auch hier ist betroffenen Personen überwiegend nicht bewusst, dass bereits „angelaufene" Werbeaktionen regelmäßig nicht mehr ohne Weiteres gestoppt werden können.

Zur Vermeidung von unnötigen Beschwerden sollten die Werbetreibenden die betroffenen Personen in einem individuellen Antwortschreiben erstens auf die Beachtung des Werbewiderspruchs und zweitens über die Tatsache, dass sie über einen möglichst genau zu benennenden kurzen Zeitraum noch Werbung erhalten können, unterrichten.

[1] Siehe dazu auch das WP 260 der Art. 29-Gruppe unter http://ec.europa.eu/newsroom/article29/news-overview.cfm

3.3
Mustertext für eine Herstellerinformation zur Datenverarbeitung im Fahrzeug

Die unabhängigen Datenschutzbehörden des Bundes und der Länder haben gemeinsam mit dem Verband der Automobilindustrie (VDA) nachfolgenden Mustertext zur Datenverarbeitung im Fahrzeug erarbeitet:

„In Ihrem Fahrzeug sind elektronische Steuergeräte verbaut. Steuergeräte verarbeiten Daten, die sie zum Beispiel von Fahrzeug-Sensoren empfangen, selbst generieren oder untereinander austauschen. Einige Steuergeräte sind für das sichere Funktionieren Ihres Fahrzeugs erforderlich, weitere unterstützen Sie beim Fahren (Fahrerassistenzsysteme), andere ermöglichen Komfort- oder Infotainment-Funktionen.

Im Folgenden erhalten Sie allgemeine Informationen zur Datenverarbeitung im Fahrzeug. Zusätzliche Informationen, welche konkreten Daten zu welchem Zweck in Ihrem Fahrzeug erhoben, gespeichert und an Dritte übermittelt werden, finden Sie unter dem Stichwort Datenschutz im unmittelbaren Zusammenhang mit den Hinweisen zu den betroffenen Funktionsmerkmalen in der jeweiligen Betriebsanleitung. Diese sind auch online und je nach Ausstattung digital im Fahrzeug verfügbar.

Personenbezug

Jedes Fahrzeug ist mit einer eindeutigen Fahrgestellnummer gekennzeichnet. Diese Fahrzeugidentifizierungsnummer ist in Deutschland über eine Auskunft beim Kraftfahrt-Bundesamt auf den gegenwärtigen und ehemaligen Halter des Fahrzeugs rückführbar. Es gibt auch weitere Möglichkeiten, aus dem Fahrzeug erhobene Daten auf den Halter oder Fahrer zurückzuführen, z. B. über das Kfz-Kennzeichen.

Die von Steuergeräten generierten oder verarbeiteten Daten können daher personenbezogen sein oder unter bestimmten Voraussetzungen personenbezogen werden. Je nachdem, welche Fahrzeugdaten vorliegen, sind gegebenenfalls Rückschlüsse z. B. auf Ihr Fahrverhalten, Ihren Standort oder Ihre Fahrtroute bzw. auf das Nutzungsverhalten möglich.

Ihre Rechte im Hinblick auf den Datenschutz

Gemäß geltendem Datenschutzrecht haben Sie bestimmte Rechte gegenüber solchen Unternehmen, die Ihre personenbezogenen Daten verarbeiten. Danach steht Ihnen ein unentgeltlicher und umfassender Auskunftsanspruch gegenüber dem Hersteller sowie Dritten (z. B. beauftragte Pannendienste oder Werkstätten, Anbieter von Online-Diensten im Fahrzeug) zu, sofern diese personenbezogene Daten von Ihnen gespeichert haben. Dabei dürfen Sie Auskunft darüber verlangen, welche Daten zu Ihrer Person zu welchem Zweck gespeichert sind und woher die Daten stammen. Ihr Auskunftsanspruch umfasst auch die Übermittlung der Daten an andere Stellen.

Weitere Informationen zu Ihren gesetzlichen Rechten gegenüber dem Hersteller (beispielsweise Ihr Recht auf Löschung oder Berichtigung von Daten) finden Sie in den jeweils anwendbaren Datenschutzhinweisen auf der Web-Site des Herstellers (inklusive Kontaktdaten des Herstellers und seines Datenschutzbeauftragten) (Fußnote 1: Hier ein direkter Verweis auf die Datenschutzhinweise auf der Web-Site des Herstellers).

Daten, die nur lokal im Fahrzeug gespeichert sind, können Sie mit fachkundiger Unterstützung z. B. in einer Werkstatt gegebenenfalls gegen ein Entgelt auslesen lassen.

Gesetzliche Anforderungen zur Offenlegung von Daten

Soweit gesetzliche Vorschriften bestehen, sind Hersteller grundsätzlich dazu verpflichtet, auf Anforderungen von staatlichen Stellen im erforderlichen Umfang beim Hersteller gespeicherte Daten im Einzelfall herauszugeben (z. B. bei der Aufklärung einer Straftat).

Staatliche Stellen sind im Rahmen des geltenden Rechts auch dazu befugt, im Einzelfall selbst Daten aus Fahrzeugen auszulesen. So können etwa aus dem Airbag- Steuergerät im Falle eines Unfalls Informationen ausgelesen werden, die helfen können, diesen aufzuklären.

Betriebsdaten im Fahrzeug

Zum Betrieb des Fahrzeuges verarbeiten Steuergeräte Daten. Dazu gehören zum Beispiel:

– Fahrzeugstatus-Informationen (z. B. Geschwindigkeit, Bewegungsverzögerung, Querbeschleunigung, Radumdrehungszahl, Anzeige geschlossener Sicherheitsgurte),
– Umgebungszustände (z. B. Temperatur, Regensensor, Abstandssensor).

In der Regel sind diese Daten flüchtig und werden nicht über die Betriebszeit hinaus gespeichert und nur im Fahrzeug selbst verarbeitet. Steuergeräte enthalten häufig Datenspeicher (unter anderem auch der Fahrzeugschlüssel). Diese werden eingesetzt, um Informationen über Fahrzeugzustand, Bauteilbeanspruchung, Wartungsbedarfe sowie technische Ereignisse und Fehler temporär oder dauerhaft dokumentieren zu können.

Gespeichert werden je nach technischer Ausstattung:

– Betriebszustände von Systemkomponenten (z. B. Füllstände, Reifendruck, Batteriestatus)
– Störungen und Defekte in wichtigen Systemkomponenten (z. B. Licht, Bremsen)
– Reaktionen der Systeme in speziellen Fahrsituationen (z. B. Auslösen eines Airbags, Einsetzen der Stabilitätsregelungssysteme)
– Informationen zu fahrzeugschädigenden Ereignissen
– bei Elektrofahrzeugen Ladezustand der Hochvoltbatterie, geschätzte Reichweite

In besonderen Fällen (z. B. wenn das Fahrzeug eine Fehlfunktion erkannt hat) kann es erforderlich sein, Daten zu speichern, die eigentlich nur flüchtig wären.

Wenn Sie Serviceleistungen (z. B. Reparaturleistungen, Wartungsarbeiten) in Anspruch nehmen, können, sofern erforderlich, die gespeicherten Betriebsdaten zusammen mit der Fahrzeugidentifikationsnummer ausgelesen und genutzt werden. Das Auslesen kann durch Mitarbeiter des Servicenetzes (z. B. Werkstätten, Hersteller) oder Dritte (z. B. Pannendienste) aus dem Fahrzeug erfolgen. Gleiches gilt für Garantiefälle und Qualitätssicherungsmaßnahmen.

Das Auslesen erfolgt in der Regel über den gesetzlich vorgeschriebenen Anschluss für OBD („On-Board-Diagnose“) im Fahrzeug. Die ausgelesenen Betriebsdaten dokumentieren technische Zustände des

Fahrzeugs oder einzelner Komponenten, helfen bei der Fehlerdiagnose, der Einhaltung von Gewährleistungsverpflichtungen und bei der Qualitätsverbesserung. Diese Daten, insbesondere Informationen über Bauteilbeanspruchung, technische Ereignisse, Fehlbedienungen und andere Fehler, werden hierfür zusammen mit der Fahrzeugidentifikationsnummer gegebenenfalls an den Hersteller übermittelt. Darüber hinaus unterliegt der Hersteller der Produkthaftung. Auch dafür verwendet der Hersteller Betriebsdaten aus Fahrzeugen, etwa für Rückrufaktionen. Diese Daten können auch dazu genutzt werden, Ansprüchen des Kunden auf Gewährleistung und Garantie zu prüfen.

Fehlerspeicher im Fahrzeug können im Rahmen von Reparatur- oder Servicearbeiten oder auf Ihren Wunsch hin durch einen Servicebetrieb zurückgesetzt werden.

Komfort- und Infotainment-Funktionen

Sie können Komforteinstellungen und Individualisierungen im Fahrzeug speichern und jederzeit ändern bzw. zurücksetzen.

Dazu gehören in Abhängigkeit von der jeweiligen Ausstattung z. B.:

– Einstellungen der Sitz- und Lenkradpositionen
– Fahrwerks- und Klimatisierungseinstellungen
– Individualisierungen wie Innenraumbeleuchtung

Sie können im Rahmen der gewählten Ausstattung selbst Daten in Infotainment-Funktionen des Fahrzeugs einbringen.

Dazu gehören in Abhängigkeit von der jeweiligen Ausstattung z. B.:

– Multimediadaten wie Musik, Filme oder Fotos zur Wiedergabe in einem integrierten Multimediasystem
– Adressbuchdaten zur Nutzung in Verbindung mit einer integrierten Freisprecheinrichtung oder einem integrierten Navigationssystem
– Eingegebene Navigationsziele
– Daten über die Inanspruchnahme von Internetdiensten

Diese Daten für Komfort- und Infotainment-Funktionen können lokal im Fahrzeug gespeichert werden oder sie befinden sich auf einem Gerät, das Sie mit dem Fahrzeug verbunden haben (z. B. Smartphone, USB-Stick oder MP3-Player). Sofern Sie Daten selbst eingegeben haben, können Sie diese jederzeit löschen.

Eine Übermittlung dieser Daten aus dem Fahrzeug heraus erfolgt ausschließlich auf Ihren Wunsch, insbesondere im Rahmen der Nutzung von Online-Diensten entsprechend der von Ihnen gewählten Einstellungen.

*[Smartphone-I*ntegration z. B. Android Auto oder Apple car play

Sofern Ihr Fahrzeug entsprechend ausgestattet ist, können Sie Ihr Smartphone oder ein anderes mobiles Endgerät mit dem Fahrzeug verbinden, sodass Sie dieses über die im Fahrzeug integrierten Bedienelemente steuern können. Dabei können Bild und Ton des Smartphones über das Multimediasystem ausgegeben werden. Gleichzeitig werden an Ihr Smartphone bestimmte Informationen übertragen. Dazu gehören je nach Art der Integration beispielsweise Positionsdaten, Tag-/Nachtmodus und weitere allgemeine Fahrzeuginformationen. Bitte informieren Sie sich in der Betriebsanleitung des Fahrzeugs-/Infotainment-Systems.

Die Integration ermöglicht eine Nutzung ausgewählter Apps des Smartphones, wie z. B. Navigation oder Musikwiedergabe. Eine weitere Interaktion zwischen Smartphone und Fahrzeug, insbesondere ein aktiver Zugriff auf Fahrzeugdaten, erfolgt nicht. Die Art der weiteren Datenverarbeitung wird durch den Anbieter der jeweils verwendeten App bestimmt. Ob und welche Einstellungen Sie dazu vornehmen können, hängt von der jeweiligen App und dem Betriebssystem Ihres Smartphones ab.]

Online-Dienste

Sofern Ihr Fahrzeug über eine Funknetzanbindung verfügt, ermöglicht diese den Austausch von Daten zwischen Ihrem Fahrzeug und weiteren Systemen. Die Funknetzanbindung wird durch eine fahrzeugeigene Sende- und Empfangseinheit oder über ein von Ihnen eingebrachtes mobiles Endgerät (z. B. Smartphone) ermöglicht. Über diese Funknetzanbindung können Online-Funktionen genutzt werden. Dazu zählen Online-Dienste und Applikationen/Apps, die Ihnen durch den Hersteller oder durch andere Anbieter bereitgestellt werden.

Herstellereigene Dienste

Bei Online-Diensten des Herstellers werden die jeweiligen Funktionen an geeigneter Stelle (z. B. Betriebsanleitung, Website des Herstellers) durch den Hersteller beschrieben und die damit verbundenen datenschutzrechtlichen Informationen gegeben. Zur Erbringung von Online-Diensten können personenbezogene Daten verwendet werden. Der Datenaustausch hierzu

erfolgt über eine geschützte Verbindung z. B. mit den dafür vorgesehenen IT-Systemen des Herstellers. Eine über die Bereitstellung von Diensten hinausgehende Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt ausschließlich auf Basis einer gesetzlichen Erlaubnis, z. B. bei einem gesetzlich vorgeschriebenen Notrufsystem, einer vertraglichen Abrede oder aufgrund einer Einwilligung.

Sie können die (zum Teil kostenpflichtigen) Dienste und Funktionen und in manchen Fällen auch die gesamte Funknetzanbindung des Fahrzeugs aktivieren oder deaktivieren lassen. Hiervon ausgenommen sind gesetzlich vorgeschriebene Funktionen und Dienste, wie etwa einem Notrufsystem.

Dienste Dritter

Sofern Sie von der Möglichkeit Gebrauch machen, Online-Dienste anderer Anbieter (Dritter) zu nutzen, unterliegen diese Dienste der Verantwortung sowie den Datenschutz- und Nutzungsbedingungen des jeweiligen Anbieters. Auf die hierbei ausgetauschten Inhalte hat der Hersteller regelmäßig keinen Einfluss.

Bitte informieren Sie sich deshalb über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten im Rahmen von Diensten Dritter beim jeweiligen Dienstanbieter.

Berlin, Februar 2018“

4. Kurzpapiere

4.1
Kurzpapier Nr. 12
Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Die nachfolgenden Erläuterungen zum Datenschutzbeauftragten (DSB) gelten sowohl für Verantwortliche als auch für Auftragsverarbeiter.

Benennung des DSB

Eine Pflicht zur Benennung eines DSB kann sich sowohl aus der DS-GVO als auch aus dem nationalen Recht ergeben. Eine Benennungspflicht kann für den Verantwortlichen, für den Auftragsverarbeiter oder für beide bestehen, je nachdem wer durch seine Tätigkeit selbst die Voraussetzungen für diese Pflicht erfüllt. Wer bisher einen DSB bestellen musste, muss in der Regel auch weiterhin einen DSB benennen.

Benennung des DSB nach Art. 37 DS-GVO

Nach Art. 37 Abs. 1 lit. a bis c DS-GVO ist auf jeden Fall ein DSB zu benennen, wenn eine der folgenden Voraussetzungen gegeben ist:

– Behörde oder öffentliche Stelle (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln)
– Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen
– Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten (Artikel 9, 10 DS-GVO)

„Kerntätigkeit“ ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwGr. 97 der DS-GVO). Zu den Kerntätigkeiten gehören danach auch alle

Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Hierzu gehören nicht die das Kerngeschäft unterstützenden Tätigkeiten wie z. B. die Verarbeitung der Beschäftigtendaten der eigenen Mitarbeiter.

Für die Definition des Begriffs „umfangreich“ können aus ErwGr 91 der DS-GVO folgende Faktoren herangezogen werden:

– Menge der verarbeiteten personenbezogenen Daten (Volumen)
– Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt)
– Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße)
– Dauer der Verarbeitung (zeitlicher Aspekt)

Sind mehrere Faktoren hoch, so kann dies für eine „umfangreiche“ Überwachung bzw. Verarbeitung sprechen.

Erfolgt eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt, handelt es sich regelmäßig nicht um eine die Benennungspflicht auslösende umfangreiche Datenverarbeitung (siehe ErwGr. 91). Unter Berücksichtigung der Umstände des Einzelfalls und der konkreten Elemente einer umfangreichen Verarbeitung im Sinne des ErwGr. 91 – beispielsweise bei einer Anzahl von Betroffenen, die erheblich über den Betroffenenkreis eines durchschnittlichen, durch ErwGr. 91 Satz 4 privilegierten Einzelarztes hinausgeht – kann eine umfangreiche Verarbeitung gegeben sein, sodass ein DSB zu benennen ist. Ungeachtet dessen ist die Benennung generell zu empfehlen, um die Einhaltung der datenschutzrechtlichen Bestimmungen zu erleichtern und damit gegebenenfalls aufsichtsbehördliche Maßnahmen zu vermeiden.

Die Regelung des Art. 37 Abs. 4 S. 1 DS-GVO sieht vor, dass DSBe auch auf freiwilliger Basis benannt werden können. Soweit keine Pflicht zur Benennung eines DSB vorliegt, kann eine freiwillige Benennung eines DSB empfehlenswert sein.

Benennung des DSB bei weiteren Verantwortlichen und Auftragsverarbeitern nach § 38 BDSG-neu

Die EU-Mitgliedstaaten haben die Möglichkeit, die Pflicht zur Benennung eines DSB in ihren nationalen Ausführungsgesetzen auf weitere Stellen auszudehnen (Art. 37 Abs. 4 S. 1 DS-GVO). Der Bundesgesetzgeber hat diesen Regelungsspielraum genutzt, um die Pflicht zur Benennung von betrieblichen

DSBen dem in Deutschland bestehenden „Status quo“ anzupassen (vgl. § 4f BDSG-alt sowie § 38 BDSG-neu).

Demnach ist eine Benennung eines DSB auch in folgenden Fällen erforderlich:

– es werden in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
– es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen oder
– es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet;

dann muss unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein DSB benannt werden.

Gemeinsamer DSB

Eine Unternehmensgruppe darf einen gemeinsamen DSB benennen (vgl. Art. 37 Abs. 2 DS-GVO). Voraussetzung hierfür ist, dass der DSB von jeder Niederlassung aus leicht erreicht werden kann. Hiervon ist auch der Fall erfasst, dass nach deutschem Recht eine Pflicht zur Benennung eines DSB besteht und dieser DSB außerhalb Deutschlands für deutsche Niederlassungen benannt wird. In diesem Zusammenhang wird jedoch empfohlen, den DSB in der Europäischen Union anzusiedeln, um die Aufgabenerfüllung in Bezug auf die DS-GVO zu erleichtern.

Behörden oder öffentliche Stellen haben die Möglichkeit, für mehrere Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen DSB zu benennen (Art. 37 Abs. 3 DS-GVO). Der Bezug auf Organisationsstruktur und Größe bedeutet auch, dass der Verantwortliche sicherstellen muss, dass der gemeinsame DSB in der Lage ist, die Aufgaben zu erfüllen, die ihm in Bezug auf sämtliche Behörden oder öffentliche Stellen übertragen wurden.

Leichte Erreichbarkeit des DSB

Es sind Vorkehrungen zu treffen, die es den betroffenen Personen oder anderen Stellen ermöglichen, den DSB leicht zu erreichen (z. B. Einrichtung einer Hotline oder eines Kontaktformulars auf der Homepage). Dem DSB muss eine Kommunikation in der Sprache möglich sein, die für die Korrespondenz mit Aufsichtsbehörden und betroffenen Personen notwendig ist.

Berufliche Qualifikation und Fachwissen

Der DSB wird aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die Aufgaben gemäß Art. 39 DS-GVO zu erfüllen, benannt.

Interner und externer DSB

Der DSB kann Beschäftigter des Unternehmens oder der Behörde sein (interner DSB) oder seine Aufgaben aufgrund eines Dienstleistungsvertrages erfüllen (externer DSB, Art. 37 Abs. 6 DS-GVO).

Form der Benennung

Da die DS-GVO lediglich von einer Benennung des DSB spricht, ist eine Schriftform – im Gegensatz zum § 4f Abs. 1 S. 1 BDSG-alt – nicht mehr vorgeschrieben. Aus Beweisgründen im Hinblick auf die Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO und Art. 5 Abs. 2 DS-GVO und zur Rechtssicherheit ist es jedoch empfehlenswert, die Benennung eines DSB in geeigneter Form zu dokumentieren. Die bereits vor Geltung der DS-GVO und dem BDSG-neu unterzeichneten Bestellungsurkunden gelten vor diesem Hintergrund fort. Die Urkunde und etwaige darin enthaltenen Zusatzvereinbarungen und Aufgabenzuweisungen sollten auf ihre Vereinbarkeit mit den neuen Regelungen der DS-GVO überprüft und ggf. angepasst werden.

Stellung des DSB und Pflichten des Verantwortlichen oder des Auftragsverarbeiters

Der Verantwortliche oder der Auftragsverarbeiter muss die Weisungsfreiheit des DSB bei der Erfüllung seiner Aufgaben sicherstellen. Der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der besondere Abberufungs- und Kündigungsschutz für DSB gemäß § 4f Abs. 3 S. 4 bis 6 BDSG-alt ist im BDSG-neu beibehalten worden (§ 6 Abs. 4 i. V. m. § 38 Abs. 2 BDSG-neu). Der DSB berichtet unmittelbar der höchsten Leitungsebene (Art. 38 Abs. 3 S. 3 DS-GVO).

Es muss nach Art. 38 DS-GVO sichergestellt werden, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Der DSB muss bei der Erfüllung seiner Aufgaben unterstützt werden, indem ihm Folgendes zur Verfügung gestellt wird:

– die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen (einschließlich Personals),
– der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie
– die zur Erhaltung seines Fachwissens erforderlichen Ressourcen.

Der DSB ist bei der Erfüllung seiner Aufgaben zur Wahrung der Geheimhaltung oder Vertraulichkeit verpflichtet. Das BDSG-neu regelt für DSB ergänzend die Pflicht zur Verschwiegenheit über die Identität der betroffenen Person, die den DSB zu Rate zieht, sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen. Darüber hinaus erstreckt § 6 Abs. 6 i. V. m. § 38 Abs. 2 BDSG-neu die Pflicht zur Wahrung der Geheimhaltung und Vertraulichkeit auf das Zeugnisverweigerungsrecht.

Der Verantwortliche kann dem DSB noch weitere Aufgaben übertragen, wobei er sicherstellen muss, dass keine Interessenkonflikte auftreten. Dies ist insbesondere anzunehmen, wenn gleichzeitig Positionen des leitenden Managements wahrgenommen werden oder die Tätigkeitsfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen.

Aufgaben des DSB

Der DSB hat nach Art. 39 DS-GVO folgende Aufgaben:

– Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutz-Pflichten (lit. a)
– Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen (lit. b)
– Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und Überwachung ihrer Durchführung (lit. c)
– Zusammenarbeit mit der Aufsichtsbehörde (lit. d) und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde (lit. e)

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO in Zusammenhang stehenden Fragen (Art. 38 Abs. 4 DS-GVO).

Risikoorientierte Aufgabenerfüllung durch den DSB

Der DSB nimmt seine Aufgaben nach Art. 39 Abs. 2 DS-GVO risikoorientiert wahr. Er trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Verantwortung für die Einhaltung der DS-GVO

Die DS-GVO stellt in Art. 24 Abs. 1 DS-GVO ausdrücklich klar, dass es die Pflicht des Verantwortlichen bzw. des Auftragsverarbeiters – und nicht die des DSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DS-GVO stehen. Gleichwohl sollte der DSB seine Tätigkeiten in angemessener Weise dokumentieren, um ggf. nachweisen zu können, dass er seinen Aufgaben (insbesondere Unterrichtung und Beratung) ordnungsgemäß nachgekommen ist.

Veröffentlichungs- und Mitteilungspflichten der Kontaktdaten des DSB

Die Kontaktdaten des DSB sind nach Art. 37 Abs. 7 DS-GVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Die Aufsichtsbehörden werden den mitteilungspflichtigen Stellen ein Formular zur Mitteilung der Kontaktdaten des DSB zur Verfügung stellen.

Rechtsfolgen bei Verstoß

Verletzungen der Vorschriften zum DSB aus Art. 37 bis 39 DS-GVO (z. B. Nicht-Benennung oder unzureichende Unterstützung des DSB) sind nach Art. 83 Abs. 4 lit. a DS-GVO mit Geldbuße bedroht.

Hinweis

Die Artikel 29-Datenschutzgruppe hat zur näheren Erläuterung der Art. 37 bis 39 DS-GVO inzwischen „*Leitlinien in Bezug auf Datenschutzbeauftragte*“ (Working Paper 243) erstellt.

4.2
Kurzpapier Nr. 13
Auftragsverarbeitung, Art. 28 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Begriff des Auftragsverarbeiters

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Der Begriff des Verantwortlichen und in der Folge die maßgebliche Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter ist in der DS-GVO nicht vollständig deckungsgleich mit dem Wortlaut des BDSG-alt. Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO die Stelle, die allein oder gemeinsam mit anderen über die Mittel und Zwecke der Verarbeitung personenbezogener Daten entscheidet. Hierbei kommt es maßgeblich auf die Entscheidung über die Verarbeitungszwecke an, während die Entscheidung über die technisch-organisatorischen Fragen der Verarbeitung auch auf den Auftragsverarbeiter delegiert werden kann (vgl. dazu schon WP 169 der Artikel 29-Gruppe, S. 17 f.). Dieses Arbeitsdokument bezieht sich zwar auf die Rechtslage unter der EU Datenschutzrichtlinie 95/46/EG [DS-RL], die grundsätzlichen Erwägungen zu diesen Fragestellungen sind aber auch für die Auslegung der DS-GVO heranziehbar.[1]

Unter BDSG-alt wurde häufig in Abgrenzung zur Auftrags-(daten-)verarbeitung die Figur der sog. Funktionsübertragung verwendet. Bei der Funktionsübertragung wurde anstelle einer Auftrags-(daten-)verarbeitung eine Übermittlung personenbezogener Daten an Dritte im Zuge des Outsourcings solcher „Funktionen"/Aufgaben angenommen, die über eine bloße Datenverarbeitung als solche hinausgehen und bei denen dem Empfänger zumindest gewisse Entscheidungsspielräume zur Aufgabenerfüllung übertragen wurden. Die Figur der Funktionsübertragung ist jedoch in der DS-GVO nicht vorgesehen. Dies ergibt sich aus der Gesamtsystematik, insbesondere aus der speziell geregelten Figur der gemeinsam Verantwortlichen (Art. 26 DS-GVO) sowie aus dem Umstand, dass gewisse Entscheidungsspielräume eines Beauftragten – innerhalb des durch den Verantwortlichen gesteckten Rahmens – bezüg-

lich der Mittel der Verarbeitung hinsichtlich der technisch-organisatorischen Fragen die Auftragsverarbeitung nicht ausschließen (WP 169, S. 17 f.).

Fortbestehende Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag

Wie schon bislang besteht auch unter der DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten im Auftrag. Allerdings legt die DS-GVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf.

Nach Art. 29 DS-GVO ist der aufgrund eines Auftrags tätige Dienstleister weisungsgebunden. Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i. S. d. Art. 4 Nr. 10 DS-GVO durch. Es besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis". Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.

Zu beachten ist, dass die Datenverarbeitung im Auftrag auch künftig keine Erlaubnis darstellt, Daten dem Auftragsverarbeiter zu offenbaren, die aufgrund gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, vertraulich zu behandeln sind (vgl. § 1 Abs. 2 S. 3 BDSG-neu). Mit dem „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen" wurden jedoch verschiedene Gesetze zu Berufsgeheimnissen novelliert. So dürfen nunmehr u. a. die in § 203 Abs. 1 oder 2 StGB genannten Berufsgeheimnisträger zum Beispiel externen Dienstleistern, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, Geheimnisse unter den Voraussetzungen des § 203 Abs. 3 und 4 StGB offenbaren. Im Gegenzug unterliegt der Auftragsverarbeiter nach § 203 Abs. 4 StGB nunmehr ebenfalls einer auch strafrechtlich sanktionierten Verschwiegenheitspflicht.

Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtsgrundlage im Sinne von Art. 6 bis 10 DS-GVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt.

Möglich ist nach der DS-GVO auch eine Auftragsverarbeitung durch Dienstleister außerhalb des EU-/EWR-Raums, wenn die zusätzlichen Anforderungen der Art. 44 ff. DS-GVO für Verarbeitungen in Drittstaaten eingehalten werden (angemessenes Schutzniveau im Drittstaat, geeignete Garantien nach Art. 46 DS-GVO wie z. B. Standarddatenschutzklauseln oder Ausnahmetatbestand nach Art. 49 DS-GVO). Auftragsverarbeiter sind Empfänger im Sinne von

Art. 4 Nr. 9 DS-GVO. Die Eigenschaft als Empfänger führt zu gesonderten Informations- (vgl. u. a. Art. 13 Abs. 1 lit. e DS-GVO) und Mitteilungspflichten (Art. 19 DS-GVO) des Verantwortlichen sowie zu Auskunftsrechten (Art. 15 DS-GVO) der betroffenen Person gegenüber dem Verantwortlichen. Empfänger von Daten müssen im Verzeichnis von Verarbeitungstätigkeiten (vgl. Art. 30 Abs. 1 lit. d DS-GVO) geführt werden.

Regelungen für Auftragsverarbeitung in Art. 28 DS-GVO

Die zentrale Vorschrift für Auftragsverarbeiter in der DS-GVO ist Art. 28, wonach dem Verantwortlichen gemäß Absatz 1 vor Auftragsvergabe zunächst eine Prüfung der Geeignetheit des Auftragsverarbeiters auferlegt wird. Der Verantwortliche darf sich danach nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden, sodass die Verarbeitung im Einklang mit der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Zum Beleg solcher Garantien können auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 DS-GVO oder Zertifizierungen nach Art. 42 DS-GVO als Faktoren herangezogen werden.

Vertrag mit dem Auftragsverarbeiter

Wie nach der bisherigen Rechtslage muss der Verantwortliche mit dem Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit schließen, der schriftlich oder in einem elektronischen Format abgefasst sein kann. Hierfür können sowohl individuelle Regelungen getroffen als auch von der EU-Kommission oder von der zuständigen Aufsichtsbehörde verabschiedete Standardvertragsklauseln verwendet werden. Für den notwendigen Inhalt des Vertrags gilt in großen Teilen das Gleiche wie bisher. Die bestehenden Verträge können daher fortgelten, wenn sie den Anforderungen der DS-GVO entsprechen oder darüber hinausgehen. Beispielsweise muss ein Vertrag zur Auftragsverarbeitung eine Regelung zur Bereitstellung der Daten beinhalten und die Einhaltung der besonderen Bedingungen für den Einsatz von Subunternehmern regeln. Unter anderem muss der Vertrag außerdem Auftragsverarbeitung vorsehen, dass der Auftragsverarbeiter die gemäß Art. 32 DS-GVO erforderlichen Maßnahmen ergreift. Da der Verantwortliche für die Rechtmäßigkeit der Verarbeitung insgesamt verantwortlich ist und bleibt (s. Art. 24 DS-GVO), ist weiterhin anzuraten, die mindestens erforderlichen technischen und organisatorischen Maßnahmen darzustellen.

Subunternehmer-Einsatz

Will sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung Subunternehmen als weiterer Auftragsverarbeiter bedienen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichem vorher mitteilen, wobei es dem Verantwortlichen vorbehalten bleibt, gegen die geplante Einbeziehung eines Subunternehmens Einspruch zu erheben. Kann nach dem Einspruch keine Einigung zwischen dem Verantwortlichen und dem Auftragsverarbeiter erreicht werden, hat der Verantwortliche die Unterbeauftragung per Weisung zu unterbinden oder die Auftragsverarbeitung zu beenden.

Der Vertrag zwischen dem Auftragsverarbeiter und dem Subunternehmer muss die gleichen vertraglichen Verpflichtungen enthalten, die der Auftragnehmer zugunsten des Auftraggebers übernommen hat.

Neue Verantwortlichkeiten und Pflichten für Auftragsverarbeiter sind insbesondere:

Die Gesamtverantwortung für die Datenverarbeitung und Nachweispflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO umfasst auch die Verarbeitung durch den Auftragsverarbeiter. Hiervon kann sich der Verantwortliche nicht durch die Beauftragung eines Auftragsverarbeiters befreien.

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers verordnungswidrig für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er nach Art. 28 Abs. 10 DS-GVO insoweit selbst als Verantwortlicher –mit allen rechtlichen Folgen, z. B. auch der Pflicht zur Erfüllung der Betroffenenrechte. Neu hinzugekommen sind in Art. 82 DS-GVO auch spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen. Demnach drohen nun Auftragsverarbeitern bei Verstößen gegen die in der DS-GVO speziell den Auftragsverarbeitern auferlegten Pflichten Schadensersatzforderungen von betroffenen Personen.

Des Weiteren besteht für Auftragsverarbeiter die neue Pflicht, künftig auch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen. Das Verzeichnis muss der Aufsichtsbehörde auf Anfrage nach Art. 30 Abs. 4 DS-GVO, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Nach Art. 33 Abs. 2 DS-GVO muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden.

Wartung und Fernzugriffe

Ist Gegenstand des Vertrages zwischen Verantwortlichem und Auftragsverarbeiter die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) und besteht in diesem Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 DS-GVO (z. B. Auslesen, Abfragen, Verwenden) ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DS-GVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen. Anders ist dies bei einer rein technischen Wartung der Infrastruktur einer IT durch Dienstleister (z. B. Arbeiten an Stromzufuhr, Kühlung, Heizung), die nicht zu einer Qualifikation des Dienstleisters als Auftragsverarbeiter und einer Anwendung von Art. 28 DS-GVO führen.

Folgen bei Verstößen

Ebenso sind die umfassenden Vorschriften über Geldbußen in Art. 83 Abs. 4, 5 und 6 DS-GVO zu berücksichtigen (bei Verstößen gegen die Vorgaben des Art. 28 DS-GVO können Geldbußen von bis zu 10.000.000 Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens verhängt werden). Diese Sanktionen können bei Verstößen nicht nur den Verantwortlichen selbst, sondern auch den Auftragsverarbeiter treffen, z. B. bei Verstößen des Auftragsverarbeiters gegen seine Verpflichtungen aus Art. 28 Abs. 2 bis 4 DS-GVO.

Anhang:

Anhang A

Auftragsverarbeitung können regelmäßig z. B. folgende Dienstleistungen sein:

– DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
– Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist

– Werbeadressenverarbeitung in einem Lettershop
– Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume dort
– Auslagerung der E-Mail-Verwaltung oder von sonstigen Datendiensten zu Webseiten (z. B. Betreuung von Kontaktformularen oder Nutzeranfragen)
– Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
– Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen
– Datenträgerentsorgung durch Dienstleister
– Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
– Zentralisierung bestimmter „Shared Services-Dienstleistungen" innerhalb eines Konzerns, wie Dienstreisenplanungen oder Reisekostenabrechnungen (jedenfalls sofern kein Fall gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO vorliegt)

Anhang B

Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines

– Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
– Inkassobüros mit Forderungsübertragung,
– Bankinstituts für den Geldtransfer,
– Postdienstes für den Brieftransport

und vieles mehr.

Anhang C

Keine Auftragsverarbeitung liegt ferner vor, wenn gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO gegeben ist, d. h. wenn mehrere Verantwortliche gemeinsam über die Verarbeitungszwecke und -mittel entscheiden. Hierunter können je nach Gestaltung eine Reihe von Verarbeitungen fallen, die bisweilen unter BDSG-alt als sog. Funktionsübertragung eingestuft wurden, etwa

– klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen,
– gemeinsame Verwaltung bestimmter Datenkategorien (z. B. „Stammdaten“) für bestimmte gleichlaufende Geschäftszwecke mehrerer Konzernunternehmen.

[1] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf

4.3
Kurzpapier Nr. 14
Beschäftigtendatenschutz

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Altes Recht = neues Recht?

In § 32 Bundesdatenschutzgesetz-alt war der Beschäftigtendatenschutz speziell geregelt. Ein umfassendes Beschäftigtendatenschutzrecht fehlte hingegen. Die DS-GVO enthält ebenfalls keine konkreten, bereichsspezifischen Regelungen. Vielmehr richtet sich der Beschäftigtendatenschutz zunächst nach den allgemeinen Regelungen der DS-GVO, die für jedes Rechtsverhältnis gelten. Allerdings enthält Artikel 88 Absatz 1 DS-GVO für den Beschäftigtendatenschutz eine sogenannte Öffnungsklausel. Sie ermöglicht den Mitgliedstaaten, spezifische Vorschriften für die Verarbeitung personenbezogener Daten im Beschäftigtenkontext zu erlassen, die den inhaltlichen Anforderungen des Artikels 88 Absatz 2 DS-GVO entsprechen müssen. Ein bislang höheres nationales Datenschutzniveau kann daher in diesem Bereich aufrechterhalten werden. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel durch Erlass des § 26 Bundesdatenschutzgesetz-neu Gebrauch gemacht.

Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes und der Länder – einschließlich der Kommunen – gelten besondere

bundes- und landesspezifische Regelungen (zum Beispiel beamtenrechtliche Vorschriften). Die Regelungen des § 26 BDSG (Bundesdatenschutzgesetz) finden dann keine Anwendung.

Inhalt § 26 BDSG-neu

I) Datenverarbeitung zum Zweck des Beschäftigtenverhältnisses

1. Grundsatz, § 26 Absatz 1 Satz 1, 1. Halbsatz BDSG-neu

§ 26 Absatz 1 Satz 1 BDSG-neu entspricht weitgehend der bisherigen Regelung des § 32 Absatz 1 Satz 1 BDSG-alt. Nach beiden Regelungen dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Insoweit gibt es keinen Unterschied zwischen der alten und der neuen Rechtslage.

2. Kollektiv-/Betriebsvereinbarungen, § 26 Absatz 1 Satz 1 und Absatz 4 BDSG-neu

In § 26 Absatz 1 Satz 1 und Absatz 4 BDSG-neu ist nunmehr ausdrücklich geregelt, dass die Verarbeitung von Beschäftigtendaten auf der Grundlage von Kollektivvereinbarungen zulässig ist. Dazu gehören Tarifverträge sowie Betriebs- und Dienstvereinbarungen (vergleiche Erwägungsgrund 155 zur DS-GVO). Die Verhandlungspartner haben die inhaltlichen Vorgaben des Artikels 88 Absatz 2 DS-GVO zu beachten. Demnach sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person zu ergreifen. Diese Vorgaben stellen sicher, dass Kollektivvereinbarungen nicht das Schutzniveau der DS-GVO absenken.

Beschäftigtendaten dürfen auch verarbeitet werden, soweit es für die Rechte und Pflichten der Interessenvertretungen der Beschäftigten erforderlich ist – unabhängig davon, ob sich diese aus einem Gesetz, Tarifvertrag beziehungsweise einer Betriebs- oder Dienstvereinbarung ergeben (§ 26 Absatz 1 Satz 1 Halbsatz 2 BDSG-neu).

II) Einwilligung

Im Beschäftigungsverhältnis kommt eine freiwillige und damit wirksame Einwilligung aufgrund des bestehenden Über-/Unterordnungsverhältnisses regelmäßig nicht in Betracht. Allerdings kannte weder das BDSG-alt noch kennen das BDSG-neu beziehungsweise die DS-GVO einen grundsätzlichen Ausschluss der Einwilligung im Beschäftigtenkontext. Die spezifische Regelung des § 26 Absatz 2 BDSG-neu enthält nunmehr jedoch restriktive Regelungen zur Frage der Freiwilligkeit einer Einwilligung. Beschäftigte können hiernach dann freiwillig in eine Datenverarbeitung einwilligen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird. Dasselbe gilt, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen.[1] Im Hinblick auf diese gesetzlichen Regelvermutungen sind aufgrund des Über-/Unterordnungsverhältnisses jedoch hohe Anforderungen an den Zweck der Einwilligung zu stellen, falls hierauf im Einzelfall eine Verarbeitung von Beschäftigtendaten gestützt werden soll.

Die Einwilligung wird in der Praxis deshalb überwiegend in Konstellationen möglich sein, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen (wie zum Beispiel bei der Gestattung privater Nutzung dienstlicher Fahrzeuge, Telefone und EDV-Geräte; Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung; Aufnahme in Geburtstagslisten).

Für die Einwilligung ist grundsätzlich die Schriftform angeordnet, um die informationelle Selbstbestimmung der betroffenen Beschäftigten abzusichern. Damit wird zugleich die Nachweispflicht des Arbeitgebers im Sinne des Artikels 7 Absatz 1 DS-GVO konkretisiert. Hinzu kommen die Pflicht des Arbeitgebers zur Aufklärung in Textform über den Zweck der Datenverarbeitung und der jederzeit mögliche Widerruf durch die Beschäftigten sowie die damit verbundenen Folgen nach Artikel 7 Absatz 3 DS-GVO.

III) Zur Aufdeckung von Straftaten

Übernommen wurde § 32 Absatz 1 Satz 2 BDSG-alt als § 26 Absatz 1 Satz 2 BDSG-neu. Danach dürfen Daten zur Aufdeckung von Straftaten verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte vorliegen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat.

Die Verarbeitung muss zur Aufdeckung erforderlich sein und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung darf nicht überwiegen. Insbesondere dürfen Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sein. Damit entspricht § 26 Absatz 1 Satz 2 BDSG-neu der bisherigen Gesetzeslage.

Die Verarbeitung darf erst erfolgen, nachdem die Anhaltspunkte vorliegen. Die vorsorgliche Verarbeitung „auf Vorrat“ ist daher unzulässig. Arbeitgeber dürfen Daten also nicht für den Fall erheben, dass später eine Straftat im Beschäftigtenverhältnis begangen werden könnte. Zudem müssen sich die Maßnahmen gegen bestimmte verdächtigte Beschäftigte richten, nicht gegen größere Gruppen von Beschäftigten.

IV) Besondere Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (vergleiche Artikel 9 Absatz 1 DS-GVO) ist im Beschäftigtenkontext unter den Voraussetzungen des § 26 Absatz 3 Satz 1 BDSG-neu möglich. Gemäß § 26 Absatz 3 Satz 2 BDSG-neu kann sich auch eine wirksame Einwilligung nach Artikel 9 Absatz 2 Buchstabe a DS-GVO in Verbindung mit § 26 Absatz 2 BDSG-neu auf diese Datenarten erstrecken, sofern sich die Einwilligung ausdrücklich auf diese Daten bezogen hat. Gemäß § 26 Absatz 4 BDSG-neu können auch Kollektivvereinbarungen Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten darstellen. Dabei haben die Verhandlungspartner die inhaltlichen Vorgaben des Artikels 88 Absatz 2 DS-GVO zu beachten. Einen Verweis auf Artikel 5 DS-GVO (Verarbeitungsgrundsätze) enthält § 26 Absatz 5 BDSG-neu. Damit wird besonders hervorgehoben, dass bei der Verarbeitung von Beschäftigtendaten geeignete Maßnahmen zu ergreifen sind. In der Gesetzesbegründung wird erläutert, dass auf diese Weise zugleich den Erfordernissen des Artikels 10 DS-GVO (Verarbeitung personenbezogener Daten über Straftaten) Rechnung getragen werden soll.

V) Verarbeitung außerhalb von Dateisystemen

Gemäß § 26 Absatz 7 BDSG-neu gilt der gesamte § 26 auch für solche Daten, die nicht in einem Dateisystem gespeichert sind und werden sollen. Damit ist der sachliche Anwendungsbereich der DS-GVO vom Gesetzgeber erweitert worden. Auf das Vorhandensein einer zumindest strukturierten Sammlung von Daten (Dateisystem) im Sinne des Artikels 4 Nr. 6 DS-GVO kommt es daher nicht an. Auch künftig unterfallen daher alle Formen der Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis – papiergebundene sowie mündliche Formen, aber auch rein tatsächliche Handlungen – den datenschutzrechtlichen Bestimmungen (vergleiche zum Beispiel Urteil des BAG vom 20.06.2013, Aktenzeichen 2 AZR 546/12). Dies können zum Beispiel handschriftliche Notizen des Arbeitgebers über Beschäftigte sein.

VI) Definition „Beschäftigte“

Die Definition des Begriffs „Beschäftigte“ in § 26 Absatz 8 BDSG-neu entspricht grundsätzlich der Bisherigen. Ausdrücklich aufgenommen wurde klarstellend, dass die Beschäftigteneigenschaft von Leiharbeitnehmern auch im Verhältnis zum Entleiher – also nicht nur zum Verleiher – vorliegt.

Anwendbarkeit DS-GVO im Übrigen

I) Allgemein

Die Reichweite des § 26 BDSG-neu und damit die verbleibende Anwendbarkeit der DS-GVO im Beschäftigtenkontext ist im jeweiligen Einzelfall zu prüfen. Hierbei ist auch der Sinn und Zweck des Artikels 88 DS-GVO in Verbindung mit § 26 BDSG-neu zu berücksichtigen.

II) Zweckänderung

Im Beschäftigtenkontext erfolgt – von Einzelfällen auf Basis einer freiwilligen Einwilligung abgesehen – die Erhebung und (Weiter-)Verarbeitung von Daten überwiegend gemäß § 26 BDSG-neu, also auf einer besonderen gesetzlichen Grundlage. Zudem erfolgt die Verarbeitung im Rahmen eines Über-/ Unterordnungsverhältnisses. Sowohl die Bewertung der Kriterien des Artikels 6 Absatz 4 DS-GVO als auch die Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f DS-GVO wird daher grundsätzlich zu dem Ergebnis kommen müssen, dass auch für neue Verwendungszwecke noch ein innerer Zusammenhang zum Beschäftigtenverhältnis im weitesten Sinne bestehen muss. Eine Verwendung zu gänzlich anderen Zwecken (zum Beispiel Verkauf an Dritte zu Werbezwecken) wird demnach ausgeschlossen sein; ein solcher Zweck ist mit dem ursprünglichen unvereinbar beziehungsweise es überwiegen in solchen Konstellationen die Interessen, Grundrechte und Grundfreiheiten der Betroffenen. Im Übrigen ist in diesem Zusammenhang auch § 24 BDSG-neu („Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen“) zu beachten.

III) Rechtsfolgen bei Verstoß

Ein Verstoß gegen die Pflichten des § 26 BDSG-neu ist gemäß Artikel 83 Absatz 5 Buchstabe d DS-GVO mit einem Bußgeldrahmen von bis zu 20 Millionen Euro (beziehungsweise 4 % des weltweiten Jahresumsatzes) sanktioniert. Strafrechtliche Regelungen enthält § 42 BDSG-neu.

Ausblick

Der Gesetzgeber hat sich vorbehalten, konkretere Vorschriften zum Beschäftigtendatenschutz zu erlassen. Ein solches Beschäftigtendatenschutzgesetz könnte unter anderem das Fragerecht bei der Einstellung von Bewerberinnen und Bewerbern, die Grenzen zulässiger Kontrollen von Beschäftigten, die Begrenzung von Lokalisierungen (GPS) und die Verwendung biometrischer Authentifizierungs- und Autorisierungssysteme zum Gegenstand haben.

[1] Im Bereich öffentlicher Stellen wird die Einwilligung im Dienst- und Arbeitsverhältnis ebenso nur unter engen Voraussetzungen in Betracht kommen, insbesondere wenn eine auf eine Einwilligung gestützte Datenverarbeitung explizit im Landesbeamtengesetz vorgesehen ist.

4.4
Kurzpapier Nr. 15
Videoüberwachung nach der Datenschutz-Grundverordnung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Die Videoüberwachung wird auch nach dem 25. Mai 2018 sowohl für die Aufsichtsbehörden als auch für die Betreiber entsprechender Anlagen ein Thema mit erheblicher praktischer Relevanz bleiben: Die DS-GVO selbst enthält keine spezifische Regelung zur Videoüberwachung. Somit ist nicht klar, in welchem Umfang die bisherigen datenschutzrechtlichen Bewertungen in der Praxis beibehalten werden können. Der ab dem 25. Mai 2018 ebenfalls in Kraft tretende § 4 des Bundesdatenschutzgesetzes (BDSG-neu, vgl. Art. 1 DSAnpUG-EU) enthält zwar eine Regelung zur Videoüberwachung öffentlich zugänglicher Räume. Ob und in welchem Umfang diese Regelung aufgrund des Anwendungsvorrangs der DS-GVO angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Welche Regelungen der DS-GVO sind für die Videoüberwachung einschlägig?

Für die Prüfung der Rechtmäßigkeit der (Daten-)Verarbeitung durch **nicht-öffentliche Stellen** ist zunächst auf die „Generalklausel" in **Art. 6 Abs. 1 S. 1 lit. f DS-GVO** abzustellen. Danach ist die Verarbeitung rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Mit Art. 2 Abs. 2 lit. c lässt die DS-GVO das bisherige sog. Haushaltsprivileg fortbestehen. Die Verordnung findet also keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (Erwägungsgrund [ErwGr.] 18).

Für öffentliche Stellen kann in bestimmten Fällen **Art. 6 Abs. 1 S. 1 lit. e, Abs. 3 DS-GVO** in Verbindung mit einem nationalen Gesetz als Rechtsgrundlage in Betracht kommen.

Soll eine Videoüberwachung auf eine Einwilligung im Sinne des **Art. 7 DS-GVO** gestützt werden, dürften die Voraussetzungen dieser Vorschrift allerdings nur in seltenen Einzelfällen erfüllt sein. Insbesondere ist das Betreten des gekennzeichneten Erfassungsbereichs einer Videokamera nicht als „eindeutig bestätigende Handlung" und auch nicht als informierte Einwilligung i. S. d. Art. 4 Nr. 11 DS-GVO zu werten.

Eine Verarbeitung biometrischer Daten (Art. 4 Nr. 14 DS-GVO) zur eindeutigen Identifizierung natürlicher Personen ist nach Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt. Auch die bloße Eignung von Videoaufnahmen für eine biometrische Analyse ist bei der Risikoabschätzung und der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen. Soweit bei der Videoüberwachung biometrische Daten zum Zweck der eindeutigen Identifizierung oder Authentifizierung einer natürlichen Person verarbeitet werden (z. B. mit einer Gesichtserkennungssoftware), gelten für solche Verarbeitungen die engen Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO. Detaillierte Hinweise hierzu sind im Kurzpapier Nr. 19 „Besondere Kategorien personenbezogener Daten" zu finden.

Welche inhaltlichen Voraussetzungen ergeben sich künftig für eine Videoüberwachungsanlage?

Die nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO durchzuführende Prüfung folgt im Wesentlichen den bereits aus dem BDSG bekannten Kriterien:

– Wahrung berechtigter Interessen
– Erforderlichkeit
– Interessenabwägung

Hinsichtlich des Tatbestandsmerkmals des „berechtigten Interesses“ kann der bisherigen Kasuistik auch weiterhin gefolgt werden. Neu ist aus deutscher Sicht allerdings die Berücksichtigung des sog. „Drittinteresses“. Als „Dritter“ kommen gemäß Art. 4 Nr. 10 DS-GVO sowohl private als auch juristische Personen in Betracht. Zu denken wäre dabei beispielsweise an die typische Konstellation in Einkaufszentren, bei der der Vermieter die Videoüberwachung auch im Interesse seiner (Laden-)Mieter, die in einer Vielzahl der Fälle nicht selbst Betroffene sind, betreibt.

Im Rahmen der Erforderlichkeitsprüfung ist nach wie vor zu fragen, ob die konkrete Videoüberwachung zur Zweckerreichung geeignet ist und ob alternative Maßnahmen, die nicht oder weniger tief in das Recht auf Schutz personenbezogener Daten eingreifen, im konkreten Einzelfall vorzuziehen sind.

Bei der Interessenabwägung ergibt sich aus ErwGr. 47 eine Relativierung des bisher strikt objektiven Ansatzes, da als Maßstab nunmehr die „vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen“ sind. Damit ist zunächst auf die subjektiven Erwartungen der betroffenen Person im Einzelfall abzustellen. Neben diesen ist aber auch zu fragen, was ein objektiver Dritter vernünftigerweise erwarten kann und darf. Entscheidend wird daher auch sein, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre typischerweise akzeptiert oder abgelehnt wird.

Insbesondere im Arbeitsverhältnis wird ein strengerer Maßstab anzulegen sein, als wenn der Betroffene als Kunde, Gast oder Passant von einer Videoüberwachung erfasst wird. In der Regel nicht zu erwarten und in diesem Zusammenhang daher nicht akzeptiert ist die Videoüberwachung z. B. im Nachbarschaftskontext sowie in Individualbereichen wie Wohnen, Sportausübung/Fitness oder ärztlichen Behandlungs- und Warteräumen. Ausnahmslos nicht akzeptiert ist die Videoüberwachung in Sanitär-und Saunabereichen. Die Prüfung wird damit deutlich vielschichtiger.

Die DS-GVO verlangt eine Abwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen bzw. Dritten als auch der Betroffenen. Ein bloßes Abstellen auf abstrakte oder auf vergleichbare Fälle

ohne Betrachtung des Einzelfalls genügt den Anforderungen der DS-GVO daher nicht.

Transparenzanforderungen und Hinweisbeschilderung

Neben der Rechtmäßigkeit der Verarbeitung fordert die DS-GVO in Art. 5 Abs. 1 lit. a ferner, dass die personenbezogenen Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Mit dieser Regelung sowie den sich aus Art. 12 ff. DS-GVO ergebenden Anforderungen sind die Transparenzpflichten stark angestiegen. Aus den Informationspflichten nach Art. 13 Abs. 1 und 2 DS-GVO ergeben sich folgende Mindestanforderungen:

– Umstand der Beobachtung – Piktogramm, Kamerasymbol
– Identität des für die Videoüberwachung Verantwortlichen – Name einschl. Kontaktdaten (Art. 13 Abs. 1 lit. a DS-GVO)
– Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit benannt, dann aber zwingend (Art. 13 Abs. 1 lit. b DS-GVO)
– Verarbeitungszwecke und Rechtsgrundlage in Schlagworten (Art. 13 Abs. 1 lit. c DS-GVO)
– Angabe des berechtigten Interesses – soweit die Verarbeitung auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO beruht (Art. 13 Abs. 1 lit. d DS-GVO)
– Dauer der Speicherung (Art. 13 Abs. 2 lit. a DS-GVO)
– Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Art. 13 Abs. 1 und 2 DS-GVO (wie Auskunftsrecht, Beschwerderecht, ggf. Empfänger der Daten)

Die weiteren Pflichtinformationen sind ebenfalls am Ort der Videoüberwachung an einer für die betroffene Person zugänglichen Stelle bereit bzw. zur Verfügung zu stellen, beispielsweise als vollständiges Informationsblatt (Aushang).

Konsequenz

Eine intransparente Videoüberwachung steht nicht im Einklang mit der DS-GVO (Art. 5, 13 DS-GVO). Die Aufsichtsbehörde kann gem. Art. 58 Abs. 2 lit. d DS-GVO den Verantwortlichen anweisen, den Mangel abzustellen oder gem. Art. 58 Abs. 2 lit. f DS-GVO die Videoüberwachung vorübergehend oder endgültig beschränken bzw. untersagen. Mangelnde Transparenz ist zudem ein Bußgeldtatbestand nach Art. 83 Abs. 5 DS-GVO.

Speicherdauer/Löschungsgebot

Die Daten der Videoüberwachung sind unverzüglich zu löschen, wenn sie zur Erreichung der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DS-GVO) oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Unter Berücksichtigung von Art. 5 Abs. 1 lit. c und e DS-GVO – „Datenminimierung“ und „Speicherbegrenzung“ – sollte demnach grundsätzlich, wie bisher auch, nach 48 Stunden eine Löschung erfolgen.

Sichere und datenschutzfreundliche Gestaltung

Bei der Beschaffung, der Installation und dem Betrieb von Videoüberwachungssystemen ist auf die sichere (Art. 32 DS-GVO) und datenschutzfreundliche (Art. 25 DS-GVO) Gestaltung zu achten. Insbesondere muss der Verantwortliche prüfen, inwieweit eine Videoüberwachung zeitlich eingeschränkt werden kann und welche Bereiche der Überwachung ausgeblendet oder verpixelt werden können. Schon bei der Beschaffung der Videotechnik ist auf „eingebauten Datenschutz“ zu achten. Nicht benötigte Funktionalität (z. B. freie Schwenkbarkeit, umfassende Überwachung per Dome-Kamera, Zoomfähigkeit, Funkübertragung, Internetveröffentlichung, Audioaufnahme) sollte von der beschafften Technik nicht unterstützt oder zumindest bei der Inbetriebnahme deaktiviert werden.

Sonderfall: Videobeobachtung in Echtzeit

Die Videoüberwachung in Echtzeit (direkte Übertragung der Bilddaten auf einen Monitor ohne Speicherung der erhobenen Daten – Kamera-Monitor-Prinzip) stellt eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten dar und ist ebenfalls nach der DS-GVO zu beurteilen.

Welche weiteren formellen Anforderungen sind zu beachten?

In dem nach Art. 30 Abs. 1 DS-GVO zu erstellenden Verarbeitungsverzeichnis soll die Videoüberwachung ausgewiesen und dokumentiert werden, welchem Zweck die Verarbeitung jeweils dient.

Ferner ist gemäß Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Videoüberwachung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies gilt nach Art. 35 Abs. 3 lit. c DS-GVO insbesondere bei einer systematischen umfangreichen (ErwGr. 91: weiträumigen) Überwachung öffentlich zugänglicher Bereiche.

Zum Inhalt der Datenschutz-Videoüberwachung nach der Datenschutzgrundverordnung-Folgenabschätzung wird auf das entsprechende Kurzpapier Nr. 5 verwiesen.

Unsere Empfehlung:

Die formellen und materiellen Anforderungen für den Einsatz einer Videoüberwachung werden mit Inkrafttreten der DS-GVO im Vergleich zum BDSG nicht abgesenkt werden. Sie bleiben vielmehr hoch und nach wie vor komplex. Daher sollten sich Betreiber von Videoüberwachungsanlagen schon zum jetzigen Zeitpunkt intensiv mit der neuen Rechtslage auseinandersetzen und prüfen, ob laufende Videoüberwachungen den geänderten Anforderungen entsprechen und fortgesetzt werden können. Dies betrifft insbesondere die gestiegenen Anforderungen an die Transparenz und an die Gestaltung der Datenverarbeitung.

In Zweifelsfällen hilft die Aufsichtsbehörde weiter.

4.5
Kurzpapier Nr. 16
Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Begriff der gemeinsamen Verantwortlichkeit

Die DS-GVO regelt in Art. 26 die „gemeinsam für die Verarbeitung Verantwortlichen“. Dieses Rechtsinstitut war zwar bereits in der EG-Datenschutzrichtlinie (RL 95/46/EG) angelegt, dort allerdings nicht detailliert ausgestaltet und spielte in Deutschland bisher – wenn überhaupt –nur eine äußerst geringe Rolle, da es im BDSG-alt nicht ausdrücklich erwähnt war. Daher wird die ausdrückliche Regelung der gemeinsamen Verantwortlichkeit in der DS-GVO gerade für die Praxis in Deutschland erhebliche Auswirkungen haben.

An eine objektiv bestehende gemeinsame Verantwortlichkeit sind zukünftig Verpflichtungen geknüpft, deren Nichteinhaltung mit Geldbuße sanktioniert werden kann (vgl. Art. 83 Abs. 4 lit. a).

Gemäß Art. 26 Abs. 1 sind mehrere Stellen „gemeinsam für die Verarbeitung Verantwortliche“, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen. Diese Definition baut konsequent auf Art. 4 Nr. 7 auf, wonach Verantwortlicher diejenige Stelle ist, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet

Keine „Privilegierungswirkung“ der gemeinsamen Verantwortlichkeit

Verantwortlichkeit ist keine Befugnis zur Datenverarbeitung. Sie stellt nur klar, wer welche Aufgaben aus der DS-GVO zu erfüllen hat. Art. 26 stellt daher weder eine Rechtsgrundlage für eine Verarbeitung durch mehrere Verantwortliche dar, noch braucht es eine Rechtsgrundlage dafür, dass sich mehrere Verantwortliche zusammenschließen. Soweit der jeweilige Verantwortliche im Rahmen der gemeinsamen Verantwortlichkeit personenbezogene Daten verarbeitet, braucht er für diese Verarbeitung eine eigene Rechtsgrundlage nach Art. 6 Abs. 1 und, soweit besondere Kategorien personenbezogener Daten verarbeitet werden, nach Art. 9 Abs. 2.

Gemeinsame Verantwortliche sind auch untereinander Empfänger im Sinne von Art. 4 Nr. 9 und können somit Gegenstand von Informationspflichten sein. Die Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ist ein eigener Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DS-GVO und bedarf als solcher einer Rechtsgrundlage. Soll eine Verarbeitung durch mehrere gemeinsam Verantwortliche etwa auf eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO gestützt werden, muss die Einwilligung daher unmissverständlich die Verarbeitung durch alle gemeinsam Verantwortlichen und mithin auch die entsprechende Weitergabe an den bzw. die anderen gemeinsam Verantwortlichen umfassen. Stellt die Übermittlung an einen anderen gemeinsamen Verantwortlichen eine Zweckänderung dar, muss außerdem nach Art. 6 Abs. 4 geprüft werden, ob die Zweckänderung erlaubt ist.

Das Institut der gemeinsamen Verantwortlichkeit dient unter anderem dazu, Haftungsfragen in Fällen zu regeln, bei denen eine Stelle gemeinsam mit mindestens einer anderen Stelle die Festlegung der Zwecke und Mittel der Verarbeitung trifft (siehe WP 169 der Artikel 29-Gruppe, S. 39). So soll verhindert werden, dass sich der einzelne an einer Datenverarbeitung Beteiligte seiner datenschutzrechtlichen Verantwortlichkeit und seiner Haftung entledigt,

wenn er zwar nicht alleine über die Zwecke und Mittel einer Verarbeitung entscheidet, jedoch neben anderen Beteiligten einen tatsächlichen Einfluss auf die Zwecke und die wesentlichen Elemente der Mittel der Verarbeitung ausübt (vgl. auch die Schlussanträge des Generalanwalts beim EuGH in der Rs. C-210/17, Rn. 54). Die Durchsetzung zivilrechtlicher Ansprüche wird mit der gesamtschuldnerischen Haftung nach Art. 26 Abs. 3 für die betroffene Person erleichtert.

Abgrenzung zu anderen Fallgestaltungen

Abzugrenzen ist die gemeinsame Verantwortlichkeit insbesondere von der **Auftragsverarbeitung** nach Art. 28 und von einer Übermittlung personenbezogener Daten an einen Verantwortlichen, bei der die Beteiligten die Zwecke und Mittel der Verarbeitung nicht gemeinsam festlegen.

Für Deutschland besteht zudem Klärungsbedarf bezüglich der **sog. Funktionsübertragung**, einer bisherigen deutschen „Besonderheit". Als Funktionsübertragung wurde unter BDSG-alt in Abgrenzung zur Auftrags-(daten-)verarbeitung das Outsourcing einer „Funktion"/Aufgabe bezeichnet, die über das Auslagern einer Datenverarbeitung als solcher hinausgeht, indem dem Empfänger ein gewisser Entscheidungsspielraum hinsichtlich der Aufgabenerfüllung eingeräumt wird. Die die „Aufgabe" übernehmende Stelle wurde in diesem Fall unter BDSG-alt als eigener Verantwortlicher angesehen; jedoch wurde in aller Regel – soweit ersichtlich – in diesem Zusammenhang üblicherweise kaum jemals eine gemeinsame Verantwortlichkeit angenommen.

Unter der DS-GVO ist für die sog. Funktionsübertragung kein Raum mehr. Dies folgt zum einen aus der in Art. 26 detailliert geregelten gemeinsamen Verantwortlichkeit, zum anderen daraus, dass gewisse Entscheidungsspielräume innerhalb des durch den Verantwortlichen gesteckten Rahmens eines Beauftragten bezüglich der Mittel der Verarbeitung die Auftragsverarbeitung nicht ausschließen. Verarbeitungen, die bislang in Deutschland als sog. Funktionsübertragung bewertet wurden, können unter der DS-GVO – je nach Fall – als Auftragsverarbeitung (Art. 28), als gemeinsame Verantwortlichkeit (Art. 26) oder aber als „normale" Übermittlung an einen anderen Verantwortlichen (ohne gemeinsame Verantwortlichkeit) eingestuft werden. Welcher Fall jeweils vorliegt, beurteilt sich allein danach, wer über die Zwecke und (zumindest wesentlichen Elemente der) Mittel der Datenverarbeitung entscheidet.

Gemeinsame Entscheidung über Zwecke und Mittel der Verarbeitung

Eine „gemeinsame Entscheidung" über die Zwecke und Mittel der Verarbeitung setzt voraus, dass jeder der Beteiligten einen bestimmenden tatsächlichen

Einfluss auf die Datenverarbeitung nimmt. Ein bestimmender Einfluss kann sich darin äußern, dass bei verschiedenen Zwecken, die von den jeweiligen Beteiligten verfolgt werden, eine Zweckverfolgung im Rahmen dieser konkreten Datenverarbeitung nicht ohne die andere möglich ist. Ein bestimmender Einfluss erfordert jedoch nicht, dass jeder der Beteiligten die umfassende Kontrolle über alle Umstände und Phasen der Verarbeitung besitzt. Auch ist keine vollständig gleichrangige Kontrolle durch alle Beteiligten erforderlich. Vielmehr kann die Beteiligung der Parteien an der Bestimmung der Zwecke und Mittel sehr verschiedene Formen annehmen und muss nicht gleichmäßig verteilt sein. Das Bestehen einer gemeinsamen Verantwortlichkeit bedeutet nicht zwingend eine gleichrangige Verantwortlichkeit. Die verschiedenen für die Verarbeitung Verantwortlichen können in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein.

Es ist denkbar, dass beteiligte datenverarbeitende Stellen nur in bestimmten Phasen der Datenverarbeitung, etwa bei der Datenerhebung, gemeinsam Verantwortliche sind. Wer welche Rolle bei der Verarbeitung einnimmt und wer für was verantwortlich ist, muss in der Vereinbarung nach Art. 26 Abs. 1 genau festgelegt sein.

So können beispielsweise der Anbieter einer IT-Anwendung oder -Plattform und die verwendende Stelle gemeinsam Verantwortliche bei der Erhebung personenbezogener Daten der Endnutzer sein, insbesondere etwa wenn der Anbieter die Daten (auch) für eigene Zwecke zu verwenden plant und insoweit einen oder mehrere Verwendungszwecke im Voraus festgelegt hat. Die Beteiligten müssen die Mittel und die (ggf. differenzierten) Zweckbestimmungen der Verarbeitung gegenseitig akzeptieren. Eine Entscheidung der verwendenden Stelle über die Zwecke und Mittel der Verarbeitung kann auch dann gegeben sein, wenn sie im Voraus durch den Anbieter festgelegte Zwecke und Mittel akzeptiert bzw. sich diesen anschließt. Eine vollständige Deckungsgleichheit der von den Beteiligten verfolgten Zwecke ist dabei nicht erforderlich, sofern die Zwecke eng zusammenhängen. Die bloße Zusammenarbeit mehrerer Stellen im Rahmen einer Kette führt als solche jedoch nicht zwingend zu einer gemeinsamen Verantwortlichkeit.

Gemeinsame Verantwortlichkeit ist nicht in der Weise möglich, dass einer der Beteiligten einer bereits bestehenden (Einzel- oder gemeinsamen) Verarbeitung für die Vergangenheit „beitritt“. Für die zukünftige Verarbeitung können indessen weitere Verantwortliche hinzutreten, sofern alle Beteiligten mit Blick auf die Zukunft gemeinsam die Zwecke und Mittel der Verarbeitung festlegen. In diesem Fall müssen alle betroffenen Personen nach Art. 26 Abs. 2 bzw. Art. 13 Abs. 3 neu informiert werden.

Eine von den Beteiligten selbst gewählte Bezeichnung oder etwaige vertragliche Vereinbarungen können (lediglich) als Hinweis auf die tatsächliche Rollenverteilung dienen (siehe WP 169 der Artikel 29-Gruppe, S. 14, Schlussanträge des Generalanwalts beim EuGH in der Rs. C-210/16, Rn. 60).

Eine gemeinsame Verantwortlichkeit kann auch in solchen Fällen vorliegen, in denen die Beteiligten das Verhältnis als Auftragsverarbeitung deklarieren, jedoch die Zwecke und Mittel der Verarbeitung auch oder sogar weitgehend vom „Auftragnehmer" vorgegeben werden.

Die Verantwortlichen haften auch ohne eine Vereinbarung nach Art. 26 Abs. 1 gemeinschaftlich.

Gemeinsame Verantwortlichkeit kann ferner vorliegen, wenn einzelne Beteiligte für bestimmte Teile bzw. Phasen einer Verarbeitung getrennt verantwortlich sind, jedoch die Daten über eine gemeinsame Plattform zusammengetragen werden (WP 169 der Artikel 29-

Gruppe, S. 25). Die gemeinsame Verarbeitung beschränkt sich dann allerdings auf den Betrieb der Plattform. Für die getrennten Verantwortungsbereiche muss die Plattform selbst bereits zwischen den einzelnen dann nicht mehr gemeinsamen Verantwortlichen trennen.

Besondere Verpflichtungen gemeinsam Verantwortlicher

Art. 26 legt den gemeinsam Verantwortlichen spezifische Pflichten auf, die über die für jeden Verantwortlichen nach der DS-GVO geltenden Pflichten hinausgehen. Dadurch soll die Transparenz und Rechtsdurchsetzung für die betroffenen Personen verbessert werden.

Die gemeinsam Verantwortlichen müssen eine Vereinbarung abschließen, in der sie in transparenter Form festlegen, wer von ihnen welche in der DS-GVO geregelten Verpflichtungen erfüllt, insbesondere die Betroffenenrechte und die Informationspflichten nach Art. 13 und 14. Diese Vereinbarung muss die tatsächlichen Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen „gebührend widerspiegeln" und das „Wesentliche" dieser Vereinbarung muss betroffenen Personen zur Verfügung gestellt werden. Die Zurverfügungstellung ergänzt die eigentliche Pflicht zur Information der betroffenen Personen nach Art. 13 und 14. „Wesentlich" und somit den betroffenen Personen zur Verfügung zu stellen ist zumindest eine nachvollziehbare Beschreibung des Zusammenwirkens und der Rollen der Beteiligten und ihrer jeweiligen Beziehung zur betroffenen Person sowie die Angabe, welcher der gemeinsam Verantwortlichen welche Betroffenenrechte und Informationspflichten erfüllen soll. Grundsätzlich dürfte es ausreichen, diese wesentlichen Elemente der Vereinbarung nach Art. 26 etwa auf einer

Website bereitzustellen (vgl. ErwGr. 58). Ungeachtet der von den gemeinsam Verantwortlichen in dieser Vereinbarung getroffenen Aufgabenteilung können jedoch betroffene Personen ihre Rechte stets bei und gegenüber jedem der gemeinsam Verantwortlichen ausüben (Art. 26 Abs. 3). Ein gut ausgearbeitetes Vertragsverhältnis zu den jeweiligen Verantwortlichkeiten als Grundlage der transparenten Vereinbarung liegt somit auch im Interesse der Verantwortlichen, die Haftungsfragen im Innenverhältnis zu klären.

Ob die Beteiligten eine Vereinbarung abgeschlossen haben, die den Anforderungen des Art. 26 entspricht, ist unerheblich dafür, ob eine gemeinsame Verantwortlichkeit vorliegt. Letztere bemisst sich allein nach den oben aufgezeigten Kriterien.

Besteht eine gemeinsame Verantwortlichkeit, ohne dass eine Vereinbarung nach Art. 26 DS-GVO getroffen wurde, können hierfür Geldbußen nach Art. 83 Abs. 4 lit. a verhängt werden.

Weitere Besonderheiten

Darüber hinaus sind im Falle gemeinsamer Verantwortlichkeit noch Besonderheiten in einigen weiteren Regelungsbereichen der DS-GVO zu beachten:

Jeder der gemeinsam Verantwortlichen haftet nach Art. 82 Abs. 4 in Verbindung mit Abs. 2 Satz 1 im Falle rechtswidriger Verarbeitung für den gesamten Schaden, sofern er nicht sein fehlendes Verschulden nachweisen kann (Art. 82 Abs. 3). Die Verantwortlichen haften auch ohne eine Vereinbarung nach Art. 26 Abs. 1 gemeinschaftlich. Diese hilft aber beim Haftungsausgleich im Innenverhältnis nach Art. 82 Abs. 5.

Fälle gemeinsamer Verantwortlichkeit können nicht selten zu einer Erhöhung der Risiken für die Rechte und Freiheiten betroffener Personen führen, sodass u. U. die Durchführung einer **Datenschutz-Folgenabschätzung** gemäß Art. 35 geboten ist.

Anwendungsfälle:

Gemeinsame Verantwortlichkeit kann angesichts der Komplexität moderner Datenverarbeitungsvorgänge bei sehr unterschiedlichen Fallgestaltungen in Betracht kommen. Es ist nicht möglich, hierzu eine abschließende Liste zu erstellen, vielmehr bedarf es einer gewissen Flexibilität, um einen effektiven Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten. Nachfolgend werden daher ohne Anspruch auf Vollständigkeit einige Fälle aufgezeigt, bei denen – je nach Gestaltung – ggf. gemeinsame Verantwortlichkeit in Betracht kommen kann:

– klinische Arzneimittelstudien, wenn mehrere Mitwirkende (z. B. Sponsor, Studienzentren/Ärzte) jeweils in Teilbereichen Entscheidungen über die Verarbeitung treffen,
– gemeinsame Verwaltung bestimmter Datenkategorien (z. B. Adressdaten) für bestimmte gleichlaufende Geschäftsprozesse mehrerer Konzernunternehmen,
– gemeinsame Errichtung einer Infrastruktur, auf der mehrere Beteiligte ihre jeweils individuellen Zwecke verfolgen, z. B. gemeinsames Betreiben einer internetgestützten Plattform für Reisereservierungen durch ein Reisebüro, eine Hotelkette und eine Fluggesellschaft,
– E-Government-Portal, bei dem mehrere Behörden Dokumente zum Abruf durch Bürger bereitstellen; der Betreiber des Portals und die jeweilige Behörde sind gemeinsam Verantwortliche (WP 169 der Artikel 29-Gruppe, Beispiel Nr. 11),
– Personalvermittlungs-Dienstleister, der für einen Arbeitgeber X Bewerber sichtet und hierbei auch bei ihm eingegangene Bewerbungen einbezieht, die nicht gezielt auf Stellen beim Arbeitgeber X gerichtet sind (WP 169, Beispiel Nr. 6),
– (je nach Gestaltung ggf.) gemeinsamer Informationspool/Warndatei mehrerer Verantwortlicher (z. B. Banken) über säumige Schuldner (WP 169, Beispiel Nr. 13).

4.6
Kurzpapier Nr. 17
Besondere Kategorien personenbezogener Daten

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Qualifizierung als besondere Kategorie personenbezogener Daten

Wie bisher werden auch künftig besondere Kategorien personenbezogener Daten bestimmt, die eines speziellen Schutzes bedürfen. Zu den bislang im Bundesdatenschutzgesetz genannten Kategorien – Angaben über die

rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit (vgl. Art. 4 Nr. 15 DS-GVO, ErwGr. 35) oder Sexualleben – treten in Art. 9 DS-GVO nun auch genetische Angaben sowie biometrische Daten (Art. 4 Nr. 13 DS-GVO, ErwGr. 34; Art. 4 Nr. 14 DS-GVO, ErwGr. 51) zur eindeutigen Identifizierung einer Person. Wurden bisher auch philosophische Überzeugungen als besonders schutzbedürftig klassifiziert, fällt diese Kategorie jetzt unter den Begriff der „weltanschaulichen" Überzeugungen, ohne dass damit inhaltliche Änderungen verbunden wären.

Besonders schutzbedürftig sind alle Angaben, die direkt oder indirekt Informationen zu den in Art. 9 DS-GVO angegebenen Datenkategorien vermitteln (z. B. Einnahme von Medikamenten, körperliche oder geistige Verfassung, regelmäßiger Besuch einer bestimmten Kirche). Andererseits wird auch künftig nicht jede mittelbare Angabe zu den besonderen Kategorien personenbezogener Daten die Anwendung der speziellen (strengen) Verarbeitungsbestimmungen nach sich ziehen – z. B. ist bloßer Alkoholkonsum im Gegensatz zu einer Alkoholabhängigkeit kein Gesundheitsdatum, der rein geographische Geburtsort keine Angabe über die rassische oder ethnische Herkunft und der einmalige Besuch eines Sakralbaus enthält keine Aussage über eine religiöse Überzeugung. Schwieriger ist die Einordnung von Lichtbildern. Sie sind erst dann als biometrisches Datum zu qualifizieren, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen (ErwGr. 51). Die Eignung von Lichtbildern zur Identifizierung im Wege biometrischer Analyseverfahren ist bei der Risikoabschätzung und der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen.

Verarbeitungsverbot mit Ausnahmevorbehalt

Art. 9 Abs. 1 DS-GVO bestimmt ein grundsätzliches Verbot der Verarbeitung von Daten dieser Kategorien. Allerdings werden in Art. 9 Abs. 2 lit. a bis j DS-GVO zugleich umfangreiche Ausnahmen von diesem Grundsatz geregelt, sodass zwar einige Veränderungen im Vergleich zur bisherigen Rechtslage zu beachten sind, die praktische Anwendung der Normen aber nur wenige Anpassungen nach sich ziehen dürfte.

Neben der ausdrücklichen Einwilligung (Art. 9 Abs. 2 lit. a DS-GVO) kommen besondere Rechtsvorschriften oder spezielle Umstände im Einzelfall als Rechtfertigung für die Verarbeitung besonders schutzbedürftiger Angaben in Betracht: Das o. g. Verarbeitungsverbot gilt gemäß Art. 9 Abs. 2 daher weiterhin nicht, wenn die Verarbeitung (lit. b bis lit. j)

b) für die Ausübung von Rechten und Pflichten aus dem Arbeits- oder Sozialrecht erforderlich ist; solche Verarbeitungen dürfen jedoch nur dann stattfinden, wenn sie nach einer Rechtsvorschrift erforderlich sind; davon umfasst sind auch Kollektivvereinbarungen wie Betriebsvereinbarungen; die Rechtsvorschriften müssen geeignete Garantien für die Grundrechte und die Interessen der betroffenen Personen vorsehen (s. a. ErwGr. 52);

c) zum Schutz lebenswichtiger Interessen einer Person erforderlich ist und diese körperlich oder rechtlich außerstande ist einzuwilligen;

d) auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung/Vereinigung/Organisation ohne Gewinnerzielungsabsicht erfolgt und sich ausschließlich auf aktuelle oder ehemalige Mitglieder oder auf Personen bezieht, die mit der Stelle regelmäßig Kontakte im Zusammenhang mit deren Tätigkeitszweck unterhalten, und die Daten nicht ohne Einwilligung nach außen weitergegeben werden;

e) Daten betrifft, die die betroffene Person offensichtlich öffentlich gemacht hat;

f) zur Rechtsverfolgung oder für die Aufgabenerfüllung der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist;

g) auf rechtlicher Grundlage aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist;

h) für Zwecke der Gesundheitsvorsorge, der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich erforderlich ist, durch Berufsgeheimnisträger erfolgt und auf einer rechtlichen Grundlage oder aufgrund eines Vertrages mit einem Angehörigen eines Gesundheitsberufes beruht;

i) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, z. B. zur Verhinderung von Epidemien oder zur Gewährleistung der Arzneimittelsicherheit, auf rechtlicher Grundlage erforderlich ist;

j) auf rechtlicher Grundlage für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO erforderlich ist.

Von den in Art. 9 Abs. 2 lit. b, g, h, i und j DS-GVO benannten Öffnungsklauseln hat der Bundesgesetzgeber in den §§ 22 Abs. 1, 27 und 28 BDSG-neu in Verbindung mit den jeweiligen konkreten spezialgesetzlichen Regelungen Gebrauch gemacht. § 22 Abs. 2 BDSG-neu enthält darüber hinaus beispielhaft aufgezählte Maßnahmen zur Wahrung der Interessen der betroffenen Personen, die jeden Verantwortlichen und damit jeden, der besondere Kategorien personenbezogener Daten verarbeitet, treffen.

Ob und wenn ja wie weit die Regelungen des BDSG-neu zur Einschränkung der Betroffenenrechte wegen des bestehenden Anwendungsvorrangs der DS-GVO angewendet werden können, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Weitere Anforderungen an die Datenverarbeitung

Zusätzlich zu den speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten sollen nach ErwGr. 51 die allgemeinen Grundsätze und andere Bestimmungen der DS-GVO, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung gelten. Bei besonders schutzbedürftigen Daten ist die Eingriffsintensität regelmäßig höher, weshalb höhere Anforderungen an die Rechtfertigung des Eingriffs zu stellen sind. Dies hat zur Folge, dass Art. 9 DS-GVO den Art. 6 DS-GVO nicht verdrängt, sondern dessen Voraussetzungen zusätzlich zu denen des Art. 6 DS-GVO vorliegen müssen.

Automatisierte Entscheidungen, die auf Kategorien besonderer Daten beruhen, sind nur zulässig, wenn die betroffene Person ausdrücklich eingewilligt hat oder die Verarbeitung auf einer speziellen Rechtsgrundlage erfolgt und aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist (Art. 22 Abs. 4 DS-GVO). Der Bundesgesetzgeber hat in § 37 Abs. 1 Nr. 2 BDSG-neu eine solche Regelung zu Entscheidungen getroffen, die auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruhen. Soweit die Entscheidung auf der Verarbeitung von Gesundheitsdaten beruht, hat der Verantwortliche nach § 37 Abs. 2 BDSG-neu angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 Satz 2 BDSG-neu vorzusehen.

Verantwortliche, die besondere Datenkategorien verarbeiten, haben in jedem Fall ein Verzeichnis aller ihrer Zuständigkeit unterliegenden Verarbeitungstätigkeiten zu führen (Art. 30 Abs. 5 DS-GVO).

Im Falle einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten muss regelmäßig eine Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 Abs. 3 lit. b DS-GVO) und es ist außerdem ein Datenschutzbeauftragter zu benennen, wenn in dieser umfangreichen Verarbeitung die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters liegt (Art. 37 Abs. 1 lit. c DS-GVO). Ausführliche Informationen dazu sind im Kurzpapier „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“ enthalten.

Anforderungen an die datenverarbeitenden Personen

Grundsätzlich dürfen unter Beachtung der in Art. 9 Abs. 2 DS-GVO genannten Voraussetzungen alle in Frage kommenden Personen die von Art. 9 Abs. 1 DS-GVO erfassten Daten verarbeiten. Soweit derartige Daten allerdings zu den in Art. 9 Abs. 2 lit. h DS-GVO genannten Zwecken (insbesondere Gesundheitsvorsorge und medizinische Versorgung) verarbeitet werden, normiert Art. 9 Abs. 3 DS-GVO spezifische Anforderungen an das Personal. Zwingende Voraussetzung für eine zulässige Verarbeitung ist dabei das Bestehen einer besonderen Geheimhaltungspflicht (Berufsgeheimnis oder Geheimhaltungsvorschrift), der die verarbeitende Person unterliegen muss.

4.7
Kurzpapier Nr. 18
Risiko für die Rechte und Freiheiten natürlicher Personen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Ziel dieses Kurzpapieres ist es, das Risiko im Kontext der DS-GVO zu definieren und aufzuzeigen, wie Risiken für die Rechte und Freiheiten natürlicher Personen bestimmt und in Bezug auf ihre Rechtsfolgen bewertet werden können. Die Eindämmung von Risiken durch Ergreifen geeigneter technischer und organisatorischer Maßnahmen ist nicht Gegenstand des Papiers.

I. Rechte und Freiheiten natürlicher Personen nach der DS-GVO (Begriffsklärung)

„Rechte und Freiheiten natürlicher Personen“ ist ein zentraler Begriff in der DS-GVO. Ziel der DS-GVO ist es gem. Art. 1 Abs. 2 DS-GVO, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Diese bestimmen sich nach der Charta der Grundrechte und Grundfreiheiten der Europäischen Union (Grundrechtecharta – GrCh) und der Europäischen Menschenrechtskonvention (EMRK). Der Begriff Rechte und Freiheiten natürlicher Personen umfasst zudem einfachgesetzliche individuelle Rechte. Er ist im Rahmen des europarechtlichen Kontextes und nicht nach rein nationalem Verständnis aus-

zulegen. Ausgangspunkt der Auslegung dieses Begriffes ist das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 GrCh, er umfasst aber grundsätzlich alle Grundrechte, die durch das Datenschutzrecht zumindest mittelbar geschützt werden. In besonderem Maße dienen auch die in Art. 5 DS-GVO normierten Grundsätze für die Verarbeitung personenbezogener Daten sowie die Vorschriften über die Betroffenenrechte (Art. 12 ff. DS-GVO) diesem Schutz.

Die Rechte und Freiheiten natürlicher Personen sind zentral bei der Abschätzung eines Risikos gemäß der DS-GVO. Jede Verarbeitung personenbezogener Daten ist mindestens eine Beeinträchtigung des Grundrechts auf den Schutz personenbezogener Daten, die durch eine Rechtsgrundlage gerechtfertigt werden muss (Art. 8 GrCh und Art. 6 DS-GVO).

II. Risiko nach der DS-GVO (Begriffsklärung)

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den ErwGr. 75 und 94 Satz 2 DS-GVO kann folgende Definition hergeleitet werden:

> Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.
>
> Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.

Gemäß ErwGr. 75 sind unter die möglichen Schäden physische, materielle und immaterielle Schäden einzuordnen. Ungerechtfertigte Beeinträchtigungen der Rechte und Freiheiten von natürlichen Personen (Grundrechtsverletzungen) sind unter die immateriellen Schäden zu rechnen. Dementsprechend wird im Folgenden allgemein von Schadensereignissen gesprochen und hierunter auch der Eintritt einer ungerechtfertigten Beeinträchtigung von Rechten und Freiheiten natürlicher Personen gefasst. Ein Schadensereignis kann das Entstehen weiterer Risiken nach sich ziehen. Unrechtmäßige Verarbeitungstätigkeiten oder Verarbeitungstätigkeiten, die nicht den Grundsätzen des Art. 5 DS-GVO entsprechen, sind in sich Beeinträchtigungen des Grundrechts auf Datenschutz und stellen daher bereits ein Schadensereignis dar. Zudem können sie zusätzliche Risiken, etwa der Diskriminierung natürlicher Personen, nach sich ziehen.

Als Beispiel hierfür kann ein fehlerhafter Eintrag in einer Datei für Hausverbote oder eine falsche Einstufung der Kreditwürdigkeit dienen – ein Verstoß gegen das Prinzip der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DS-GVO –, die darüber hinaus zu finanziellen Folgeschäden und Rufschädigungen führen können.

Schäden können sich grundsätzlich ergeben aus:

a. der geplanten Verarbeitung selbst,
b. eigenverantworteten und
c. fremdverursachten Abweichungen von der geplanten Verarbeitung (z. B. Drittwirkung, Naturkatastrophen, Hardwaredefekte ...)

III. Risiko und Rechtsfolgen

Die DS-GVO verwendet die Unterscheidungen „Risiko“ und „hohes Risiko“ (z. B. ErwGr. 76). Daneben wird die Formulierung „voraussichtlich nicht zu einem Risiko“ führend verwendet (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DS-GVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden. Ziel der Risikobeurteilung ist es daher, die Risiken nach den Abstufungen „geringes Risiko“, „Risiko“ und „hohes Risiko“ zu bestimmen.

Das Risiko mit Blick auf Rechtsfolgen unter der DS-GVO ist relevant insbesondere bei:

– Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 Abs. 1 DS-GVO)
– Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DS-GVO)
– Sicherheit der Verarbeitung (Art. 32 DS-GVO)
– Umgang mit einer Verletzung des Schutzes personenbezogener Daten (Art. 33, 34 DS-GVO)
– Datenschutz-Folgenabschätzung und vorherige Konsultation (Art. 35, 36 DS-GVO

IV. Risikobeurteilung

Zur Risikobeurteilung sind die im Folgenden beschriebenen Phasen zu durchlaufen:

1. Risikoidentifikation
2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

3. Zuordnung zu Risikoabstufungen

Grundlage einer Risikobeurteilung muss eine konkrete Beschreibung des zugrunde gelegten Sachverhalts sein, für den das Risiko abgeschätzt werden soll.

1. Risikoidentifikation

Zur Identifikation von Datenschutzrisiken bietet es sich an, von folgenden Fragen auszugehen:

a. Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten bewirkt werden?
b. Wodurch, d. h. durch welche Ereignisse kann es zu dem Schaden kommen?
c. Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

zu a.) Schäden für natürliche Personen

Schäden können nach der DS-GVO physischer, materieller oder immaterieller Natur sein (ErwGr. 75 Satz 1). Der Schadensbegriff ist somit in einem umfassenden Sinne zu verstehen und nicht auf monetär bezifferbare Schäden begrenzt.

Es müssen die negativen Folgen der geplanten Verarbeitung selbst betrachtet werden. Dazu gehören auch Einschränkungen von Rechten und Freiheiten, beispielsweise wenn betroffene Personen aus Angst vor Nachteilen auf die Ausübung ihrer Rechte verzichten (z. B. Verzicht auf Teilnahme an einer Demonstration aufgrund umfangreicher Überwachung).

Auch negative Folgen von Abweichungen von der geplanten Verarbeitung müssen betrachtet werden (z. B. Datenzugang durch unbefugte Personen oder Stellen, unbefugte Offenlegung oder Verknüpfung von Daten, zufällige Vernichtung von Daten, Ausfall oder Einschränkungen von vorgesehenen Prozessen, unbeabsichtigte oder vorsätzliche unbefugte Veränderung der Daten, Nichterfüllung eines Auskunftsanspruchs). Die Abweichungen können zu einer unrechtmäßigen oder einer die Datenschutzgrundsätze verletzenden Verarbeitung führen.

Durch jede Verarbeitung personenbezogener Daten erfolgt mindestens eine Beeinträchtigung des Grundrechts auf Schutz personenbezogener Daten (vgl. Art. 8 GrCh). Daneben können weitere Grundrechte betroffen sein, wie z. B. die Achtung des Familienlebens in Art. 7 GrCh oder die Meinungs- und Versammlungsfreiheit in Art. 11 und 12 GrCh oder das Recht auf Nichtdis-

kriminierung in Art. 21 GrCh. Diese Beeinträchtigungen führen zu Schäden, wenn sie nicht gerechtfertigt sind.

Letztlich müssen alle denkbaren negativen Folgen der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, ihre wirtschaftlichen, finanziellen und immateriellen Interessen, ihren Zugang zu Gütern oder Dienstleistungen, für ihr berufliches und gesellschaftliches Ansehen, für ihren gesundheitlichen Zustand und für alle ihre sonstigen legitimen Interessen betrachtet werden.

Beispiele möglicher Schäden sind unter anderem:

– Diskriminierung
– Identitätsdiebstahl oder -betrug
– finanzieller Verlust
– Rufschädigung
– wirtschaftliche oder gesellschaftliche Nachteile
– Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen
– Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten
– Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte
– körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten

zu b.) Ereignisse

Für jeden bereits identifizierten möglichen Schaden werden die Ereignisse ermittelt, die zu seiner Verwirklichung führen können. Diese bestehen in der Nichteinhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO sowie der Nichtgewährung der Betroffenenrechte nach Art. 12 ff. DS-GVO, insbesondere:

– unbefugte oder unrechtmäßige Verarbeitung
– Verarbeitung wider Treu und Glauben
– für den Betroffenen intransparente Verarbeitung
– unbefugte Offenlegung von und Zugang zu Daten
– unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
– Verweigerung der Betroffenenrechte
– Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken
– Verarbeitung nicht vorhergesehener Daten

– Verarbeitung nicht richtiger Daten
– Verarbeitung über die Speicherfrist hinaus

Bei Schäden, die sich aus der Verarbeitung selbst ergeben, besteht das Ereignis in eben dieser Verarbeitung.

zu c.) Risikoquellen

Ein relevanter Teil der Risikoquellen ist dem Bereich des Verantwortlichen oder Auftragsverarbeiters und der von diesen plangemäß durchgeführten Verarbeitung zuzuordnen. Dabei ist auch in Betracht zu ziehen, inwieweit Personen im Bereich des Verantwortlichen oder etwaiger Auftragsverarbeiter bewusst oder unbeabsichtigt den für die Verarbeitung vorgesehenen Rahmen überschreiten könnten (z. B. eine Vertriebsabteilung, die die Zweckbindung von Kundendaten ändern könnte, etwa um eine Zielvorgabe zum Umsatz zu erfüllen).

Ein weiteres Beispiel sind Beschäftigte, die vorsätzlich gegen Anweisungen zum Umgang mit personenbezogenen Daten verstoßen oder vorsätzlich in Verfolgung eigener Interessen unbefugt handeln.

Des Weiteren sind Risiken durch unbefugte Angreifer wie Cyberkriminelle zu berücksichtigen. Risikoquellen können ggf. auch staatliche Stellen sein, die sich unbefugt Zugang verschaffen können. Schließlich können Risikoquellen bei Kommunikationspartnern liegen, mit denen personenbezogene Daten befugt ausgetauscht werden, oder bei Herstellern und Dienstleistern, die Informationstechnik einschließlich der mit ihr verwendeten Software, die für die Verarbeitung personenbezogener Daten oder in ihrem Umfeld eingesetzt wird, bereitstellen oder warten.

Schließlich sind technische Fehlfunktionen und äußere Einflüsse, z. B. durch höhere Gewalt, als Risikoquellen zu berücksichtigen.

2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

Für jeden möglichen Schaden werden die Eintrittswahrscheinlichkeit und Schwere abgeschätzt. Diese lassen sich nur in ganz wenigen Ausnahmefällen mathematisch fassen.

Dennoch verlangt die DS-GVO, das Risiko anhand objektiver Kriterien zu beurteilen (ErwGr. 76). Insbesondere in Fällen immaterieller Schäden, wie z. B. einer Rufschädigung, muss auch – auf Basis objektiver Kriterien – beurteilt werden, als wie schwerwiegend die möglichen negativen Folgen für die Lebensführung der betroffenen Personen einzustufen sind.

Eine Möglichkeit für die Bemessung eines Risikos besteht darin, eine Abstufung der Ausprägungen von Schwere und Eintrittswahrscheinlichkeit eines möglichen Schadens auf einer Skala – mit beispielsweise vier Ausprägungen – darzustellen.

Sowohl für die Differenzierung der Eintrittswahrscheinlichkeit als auch für mögliche Schäden könnten jeweils folgende Abstufungen verwendet werden:

– geringfügig
– überschaubar
– substanziell
– groß

Die Einordnung in die Stufen ist zu begründen.

Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann.

Handelt es sich zum Beispiel bei dem Schadensereignis um die ungewollte Offenlegung der sexuellen Orientierung einer Person, so ist die Wahrscheinlichkeit sowohl dieser Offenlegung als auch der hieraus resultierenden weiteren Schäden einzuschätzen.

Die Wahrscheinlichkeiten der verschiedenen Wege, die zu einer solchen Offenlegung führen können, summieren sich hierbei. Im genannten Beispiel gehören unzureichende Vorkehrungen des Verantwortlichen, sorgloser Umgang von Beschäftigten unter seiner direkten Verantwortung mit der Information, technische Fehlfunktionen oder Ausspähung durch Dritte zu den zu betrachtenden Wegen.

Die Schwere des möglichen Schadens

Die Schwere eines möglichen Schadens muss in jedem Einzelfall insbesondere unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden (ErwGr. 76). Wesentliche Faktoren sind insbesondere:

– Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DS-GVO, bei denen die DS-GVO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht;

– Verarbeitung von Daten schützenswerter Personengruppen (z. B. Kinder, Beschäftigte);
– Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten wie z. B. eindeutigen Personenkennzahlen im Vergleich zu pseudonymisierten Daten;
– automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z. B. Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für betroffene Personen getroffen werden (vgl. Art. 35 Abs. 3 lit. a DS-GVO);
– wenn der Schaden nicht oder kaum reversibel ist oder die betroffene Person nur wenige oder beschränkte Möglichkeiten hat, die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen oder sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat;
– wenn die Verarbeitung eine systematische Überwachung ermöglicht;
– die Anzahl der betroffenen Personen, die Anzahl der Datensätze und die Anzahl der Merkmale in einem Datensatz sowie die geographische Abdeckung, die mit den verarbeiteten Daten erreicht wird.

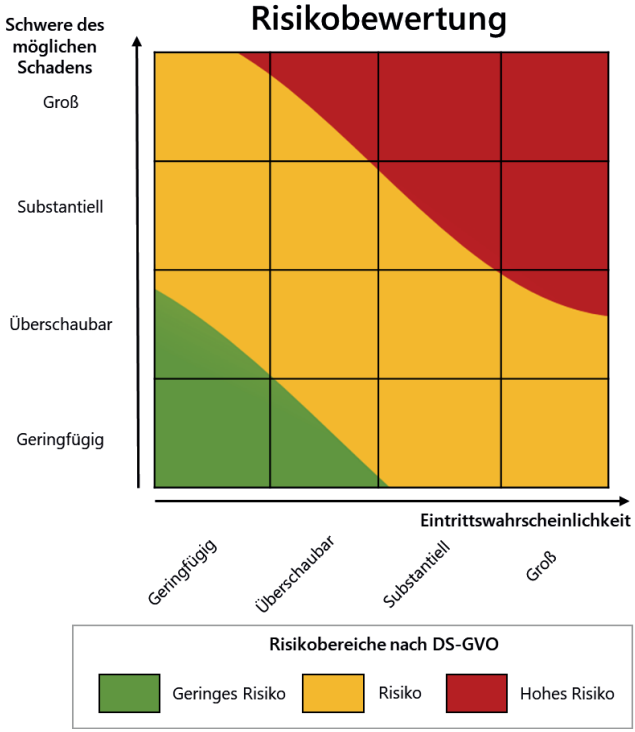
3. Zuordnung zu Risikoabstufungen

Nachdem die Eintrittswahrscheinlichkeit und die Schwere möglicher Schäden bestimmt wurden, müssen diese den Risikoabstufungen „geringes Risiko“, „Risiko“ und „hohes Risiko“ zugeordnet werden. Wie diese Abbildung konkret erfolgt, wird in der DS-GVO nicht näher beschrieben – es besteht daher grundsätzlich Spielraum für verschiedene Modelle.

Als Risiko der Verarbeitung insgesamt ist grundsätzlich die höchste Risikoklasse der Einzelrisiken anzunehmen. Sollten in dieser Risikoklasse viele Einzelrisiken vorhanden sein, kann es jedoch im Einzelfall erforderlich sein, eine höhere Risikoklasse anzunehmen.

Risikomatrix

Für die Abschätzung des Risikos der Verarbeitung gemäß der Eintrittswahrscheinlichkeit und der Schwere des möglichen Schadens kann die folgende Matrix verwendet werden:



Bei der Abschätzung des Risikos anhand der Matrix können Fälle eintreten, in denen der Eintritt des Schadens relativ wahrscheinlich ist oder der potenzielle Schaden besonders schwer wiegen würde und somit Grenzbereiche zwischen den Risikobereichen betroffen sein können. Hier sind in den Feldern der Matrix zwei Farben eingetragen. Dies macht deutlich, dass in diesen Grenzfällen eine Einzelfallbetrachtung notwendig ist. Diese kann im Zweifel zu dem Schluss kommen, dass trotz des Ergebnisses der generischen Abschätzung anhand der Matrix der Einzelfall als so schwerwiegend erscheint, dass dennoch ein hohes Risiko gegeben ist. Umgekehrt kann im Einzelfall z. B. auch ein geringfügiger möglicher Schaden, der eine überschaubare Eintrittswahrscheinlichkeit hat, ein geringes Risiko darstellen.

Mit der bis zu diesem Punkt beschriebenen Vorgehensweise wird das Ausgangsrisiko einer Datenverarbeitung unter Berücksichtigung der Umstände der Verarbeitung bestimmt.

V. Eindämmung des Risikos

Im Wege der Datenschutz-Folgenabschätzung oder – falls voraussichtlich kein hohes Risiko vorliegt – in einem vereinfachten Verfahren sind als nächster Schritt die Maßnahmen zur angemessenen Eindämmung der Risiken zu ermitteln.

Grundsätzlich ist das Risiko einer Verarbeitung mittels Abhilfemaßnahmen einzudämmen. Oft wird dies mit dem Stand der Technik entsprechenden technischen und organisatorischen Maßnahmen (TOMs) zu erreichen sein, die geeignet sind, die Rechte und Freiheiten der betroffenen natürlichen Personen angemessen zu gewährleisten, indem die Eintrittswahrscheinlichkeit und/oder die Schwere des möglichen Schadens eingedämmt werden. Dazu gehören auch Maßnahmen zur Eindämmung unerwünschter Ereignisse (z. B. Angriffe von Cyberkriminellen), wie die klassischen Security-Maßnahmen aus der Informationssicherheit, die jedoch im Hinblick auf den Schutz der betroffenen Personen und nicht der Verantwortlichen zu bewerten sind.

VI. Restrisiko

Das nach Umsetzung dieser Maßnahmen verbleibende Risiko wird als Restrisiko bezeichnet. Wenn dieses Restrisiko als hoch einzustufen ist, besteht die Pflicht zur vorherigen Konsultation gemäß Art. 36 DS-GVO.

Der Verantwortliche muss genau prüfen (und gem. Art. 5 Abs. 2 DS-GVO als Nachweis für die Erfüllung der Anforderungen der DS-GVO dokumentiert haben), ob er alle ihm nach dem Grundsatz der Verhältnismäßigkeit möglichen Maßnahmen zur Eindämmung des Risikos ergriffen hat, bevor er mit einer Verarbeitung beginnt.

Nach Umsetzung der Abhilfemaßnahmen müssen diese auf ihre Wirksamkeit getestet und kontinuierlich überwacht werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

Fazit

Die objektive Ermittlung und Beurteilung des Risikos einer Verarbeitung personenbezogener Daten im o. g. Sinn ist erforderlich, um festzustellen, wie die Rechte und Freiheiten natürlicher Personen wirksam geschützt werden.

4.8
Kurzpapier Nr. 19
Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung des Europäischen Datenschutzausschusses.

Was regelt die Datenschutz-Grundverordnung (DS-GVO)?

Nach Artikel 29 DS-GVO dürfen Beschäftigte eines Verantwortlichen (eines Unternehmens, eines Vereins, eines Verbands, eines Selbstständigen, einer Behörde und so weiter) oder eines Auftragsverarbeiters personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Ergänzend dazu regelt Artikel 32 Absatz 4 DS-GVO, dass der Verantwortliche oder Auftragsverarbeiter Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen (insbesondere seine Beschäftigten), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten (es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor). Für den Fall der Auftragsverarbeitung bestimmt Artikel 28 Absatz 3 Satz 2 Buchstabe b DS-GVO, dass der Auftragsverarbeiter gewährleisten muss, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben (soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; Letzteres gilt zum Beispiel für privatärztliche, steuerberaterliche oder anwaltliche Verrechnungsstellen).

Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten“ sind, trifft inhaltlich diese „verpflichtende Unterrichtung“ (im Folgenden: Verpflichtung) auch die Verantwortlichen und ihre Beschäftigten. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und gegebenenfalls der Aufsichtsbehörde nachweisen), ist nicht verbindlich geregelt. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. Ein Muster für eine solche Verpflichtung finden Sie in der Anlage.

Zu was soll verpflichtet werden?

Die Verpflichtung von Beschäftigten zur Wahrung des Datengeheimnisses und zur Beachtung der datenschutzrechtlichen Anforderungen ist ein wichtiger Bestandteil der Maßnahmen, die erforderlich sind, damit ein Verantwortlicher (siehe Artikel 5 Absatz 2 und Artikel 24 Absatz 1 DS-GVO) oder ein Auftragsverarbeiter (siehe Artikel 28 Absatz 3 Satz 2 Buchstabe b DS-GVO) die Einhaltung der Grundsätze der DS-GVO sicherstellen und nachweisen kann („Rechenschaftspflicht“). Diese Grundsätze der DS-GVO, festgelegt in Artikel 5 Absatz 1 DS-GVO, beinhalten im Wesentlichen folgende Pflichten:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Kernelement der Maßnahme ist, dass die Beschäftigten auf die Einhaltung betrieblicher Weisungen verpflichtet werden. Die Form der jeweiligen Weisung ist dabei nachrangig. In Frage kommen neben Einzelanweisungen der Vorgesetzten insbesondere Betriebsvereinbarungen und allgemeine Dienstanweisungen. Außerdem kann Prozessbeschreibungen (zum Beispiel aus dem Qualitätsmanagement), Ablaufplänen sowie Dokumentationen (zum Beispiel Verzeichnis von Verarbeitungstätigkeiten) und Handbüchern Weisungscharakter zukommen.

Wer muss verpflichtet werden?

Der Kreis der zu verpflichtenden Personen (die DS-GVO spricht insoweit von „unterstellten natürlichen Personen“) ist aufgrund der Bedeutung dieser Regelung weit auszulegen. Insbesondere sind ergänzend zum regulären Mitarbeiterstamm auch Auszubildende, Praktikanten, Referendare, Leiharbeiter und ehrenamtlich Tätige mit einzubeziehen.

Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.

Wann muss die Verpflichtung erfolgen?

Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen. Sie sollte daher möglichst (spätestens) am ersten Arbeitstag vorgenommen werden.

Wie muss eine Verpflichtung erfolgen?

Zuständig für die Verpflichtung ist die Unternehmensleitung, der Inhaber einer Firma oder ein von diesen Beauftragter. Selbst wenn, wie oben ausgeführt, die DS-GVO keine bestimmte Form der Verpflichtung vorschreibt, sollte schon aus Nachweisgründen ein spezielles Formular verwendet werden, wobei die Verpflichtung schriftlich oder in einem elektronischen Format erfolgen kann.

Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten. Die Beschäftigten sind – möglichst anhand typischer Fälle – darüber zu informieren, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen. Mit der Verpflichtung nach der DS-GVO können auch andere Geheimhaltungsvereinbarungen kombiniert werden, zum Beispiel zum Betriebs-, Telekommunikations- oder Steuergeheimnis. Aus Nachweisgründen im Rahmen der Rechenschaftspflicht nach der DS-GVO ist es wichtig, die Verpflichtung ausreichend zu dokumentieren.

Reicht die einmalige datenschutzrechtliche Verpflichtung?

Zur laufenden Sensibilisierung der Beschäftigten für Fragen des Datenschutzes empfiehlt es sich, in regelmäßigen Zeitintervallen im Rahmen von Schulungen oder in schriftlichen Hinweisen, zum Beispiel in der Betriebszeitung, daran zu erinnern, dass die Beschäftigten verpflichtet worden sind und welche Bedeutung dieser Verpflichtung zukommt. Wenn ein Arbeitsplatzwechsel im Unternehmen oder in der Behörde erfolgt, der mit einem Aufgabenwechsel

verbunden ist, sollte dies immer auch zum Anlass genommen werden, die Verpflichtung zu überprüfen und gegebenenfalls anzupassen.

Anlage/Musterbeispiel für eine schriftliche Verpflichtung[1]:

Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr _____

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Artikel 5 Absatz 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen[2]:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter

Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Personenbezogene Daten dürfen daher nur nach Weisung des Verantwortlichen verarbeitet werden. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher[3].

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- beziehungsweise Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen

[1] Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.

[2] Der Inhalt der Verpflichtung ist im Einzelfall anzupassen. So können bestimmte Aufgaben und Tätigkeiten zusätzliche Unterrichtungen erfordern, etwa zum Beschäftigten- oder Sozialdatenschutz, zum Telekommunikationsgeheimnis und so weiter.

[3] Die Aufzählung ist im Einzelfall anzupassen. So können weitere Unterlagen Weisungscharakter haben oder aufgezählte Typen für einzelne Verantwortliche nicht von Bedeutung sein.

5. Entschließung der 36. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 16.10.2018

5.1
Soziale Teilhabe braucht konsequente Veröffentlichung von Verwaltungsvorschriften!

Eine offene und transparente Verwaltungskultur ist eine Voraussetzung dafür, dass sich Bürgerinnen und Bürger und Staat auf Augenhöhe begegnen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Sozialleistungsträger auf, Verwaltungsvorschriften antragsunabhängig, zeitnah und benutzerfreundlich zu veröffentlichen, soweit sie dazu nicht bereits gesetzlich verpflichtet sind.[1]

Soziale Teilhabe aller Menschen in unserer Gesellschaft folgt aus dem im Grundgesetz verankerten Sozialstaatsprinzip. Ausdruck dieses Prinzips ist ein soziales Sicherungssystem, das durch Sozialleistungen auf Grundlage der Sozialgesetzbücher einen Grundstandard an sozialer Sicherheit gewährleisten soll. Nur informierte Bürgerinnen und Bürger können die sie betreffenden Entscheidungen von Sozialleistungsträgern verstehen, Ansprüche geltend machen, aber auch Pflichten wahrnehmen.

Alle Sozialleistungsträger bedienen sich Verwaltungsvorschriften, um innerhalb ihrer Behörde eine einheitliche Bearbeitungs- bzw. Entscheidungspraxis sicherzustellen. Verwaltungsvorschriften sind interne Weisungen, die regeln, wie Gesetze auszulegen und anzuwenden sind. Zwar binden Verwaltungsvorschriften unmittelbar nur die Verwaltung selbst; die auf ihrer Grundlage getroffenen Entscheidungen wirken aber nach außen. Verwaltungsvorschriften sind daher bekannt zu geben, damit „der Betroffene (...) sich des Inhalts der durch sie für ihn begründeten Rechte und Pflichten vergewissern“[2] kann. So agieren in diesem Bereich etwa die Bundesagentur für Arbeit sowie die Deutsche Rentenversicherung, die aktuelle Weisungen veröffentlichen. Viele andere Sozialleistungsträger geben die Informationen hingegen allenfalls auf Antrag heraus.

[1] Gesetzliche Verpflichtungen bestehen derzeit in: Hamburg, Bremen, Rheinland-Pfalz, Schleswig-Holstein (ab 1.1.2020).

[2] Urteil des Bundesverwaltungsgerichts vom 25.11.2004, Az. 5 CN 1.03.

Sachwortverzeichnis

ERSTER TEIL: BERICHT ZUM DATENSCHUTZ

ZWEITER TEIL: BERICHT ZUR INFORMATIONSFREIHEIT