Sechsundvierzigster Tätigkeitsbericht

des

Hessischen Datenschutzbeauftragten

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2017

gemäß § 30 des Hessischen Datenschutzgesetzes

Inhaltsverzeichnis

Abkürzungsverzeichnis zum 46. Tätigkeitsbericht

a. a. O.	am angegebenen Ort
a. E.	am Ende
a. F.	alte Fassung
Abb.	Abbildung
Abs.	Absatz
AD	Active Directory
ADV	Auftragsdatenverarbeitung
AdVermiG	Adoptionsvermittlungsgesetz
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
App	Application Software
Art.	Artikel
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BDSG-neu	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 30.06.2017
BFZ	Beratungs- und Förderzentren
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BImSchV	Bundesimmissionsschutzverordnung
BRDrucks.	Bundesratsdrucksache
BTDrucks.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des BVerfG
BvR	Registerzeichen beim BVerfG für Verfahren über Verfassungsbeschwerden nach Art. 93 Abs. 1 Nr. 4a GG sowie über Kommunalverfassungsbeschwerden nach Art. 93 Abs. 1 Nr. 4b GG
bzw.	beziehungsweise
ca.	circa
CERT	Computer Emergency Response Team Computersicherheits-Ereignis- und Reaktionsteam
d. h.	das heißt
D.C.	District of Columbia
DAkkS	Deutsche Akkreditierungsstelle GmbH
DB-Lounges	Deutsche Bahn-Lounges
DigLu	Digitales Lernen unterwegs
DSAnpUG-EU	Datenschutz-Anpassungs- und Umsetzungsgesetz-EU
DSFA	Datenschutzfolgenabschätzung
DS-GVO oder DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DVB-T	Digital Video Broadcasting-Terrestrial
DVD	Digital Video Disc
e. V.	eingetragener Verein

eAT	elektronischer Aufenthaltstitel
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EG	Erwägungsgrund
eID	elektronischer Identitätsnachweis
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
FCA	Facebook Custom Audience
GEMA	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
GlüStV	Glücksspielstaatsvertrag
grds.	grundsätzlich
HArchivG	Hessisches Archivgesetz
HbbTV	Hybrid broadcast broadband Television
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HGlüG	Hessisches Glücksspielgesetz
HIS	Hinweis- und Informationssystem
HMdIS	Hessisches Ministerium des Innern und für Sport
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
i. d. F.	In der Fassung vom
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
IHK	Industrie- und Handelskammer
insb.	insbesondere
ISMS	IT-Sicherheits-Managementsystem
IT	Informationstechnik
Kfz-Kennzeichen	Kraftfahrzeugkennzeichen
KIS	Krankenhausinformationssystem
KMK	Kultusministerkonferenz
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
lit.	littera
LTDrucks.	Landtagsdrucksache
m. E.	meines Erachtens
MDM	Mobiles Device Management

Nr.	Nummer
o. Ä.	oder Ähnliches
o. a.	oben angegeben/angegebene/angegebener/angegebenes
o. g.	oben genannt/genannte/genannter/genanntes
OH KIS	Orientierungshilfe Krankenhausinformationssysteme
OWiG	Gesetz über Ordnungswidrigkeiten
PaßG	Passgesetz
PAuswG	Personalausweisgesetz
PCLOB	Privacy and Civil Liberties Oversight Board
PVR	Personal Video Recorder
Rdnr.	Randnummer
S.	Seite *oder* Satz
s.	siehe
s. o.	siehe oben
s. u.	siehe unten
SchfHwG	Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk
SGB	Sozialgesetzbuch
sog.	sogenannte/sogenannter/sogenanntes
SSA	Staatliches Schulamt
StAnz.	Staatsanzeiger für das Land Hessen
StPO	Strafprozessordnung
TOMs	technische und organisatorische Maßnahmen
u. a.	unter anderem
u. Ä.	und Ähnliche/Ähnlicher/Ähnliches
ugs.	umgangssprachlich
u. U.	unter Umständen
U.S.	Vereinigte Staaten von Amerika
UAbs.	Unterabsatz
Urt.	Urteil
US(A)	Vereinigte Staaten von Amerika
USA	Vereinigte Staaten von Amerika
USB	Universal Serial Bus
usw.	und so weiter
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom
vgl.	vergleiche
VIP	very important person – sehr wichtige Person
VPN	Virtual Private Network
VÜ	Videoüberwachung
wp oder WP	Workingpaper oder Working Paper

WP 29	Article 29 Working Party (Artikel 29-Arbeitsgruppe)
z. B.	zum Beispiel
Ziff.	Ziffer
ZPM	Zentralstelle Personalmanagement
ZPO	Zivilprozessordnung
ZPÜ	Zentralstelle für private Überspielungsrechte

Register der Rechtsvorschriften

Gesetz/Vorschrift	Fundstelle(n)
AdVermiG	Gesetz über die Vermittlung der Annahme als Kind und über das Verbot der Vermittlung von Ersatzmüttern (Adoptionsvermittlungsgesetz) i. d. F. vom 22.12.2001 (BGBl. 2002 I S. 354), zuletzt geändert durch Gesetz vom 20.11.2015 (BGBl. I S. 2010, 2014)
AVBWasserV	Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser vom 20.06.1980 (BGBl. I S. 750, 1067), zuletzt geändert durch Verordnung vom 11.12.2014 (BGBl. I S. 2010)
BDSG	Bundesdatenschutzgesetz i. d. F. der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 31.10.2017 (BGBl. I S. 3618)
BDSG-neu	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30.06.2017 (BGBl. I S. 2097)
BImSchV	Erste Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Verordnung über kleine und mittlere Feuerungsanlagen – 1. BImSchV) vom 26.01.2010 (BGBl. I S. 38), zuletzt geändert durch Gesetz vom 10.03.2017 (BGBl. I S. 420)
BMG	Bundesmeldegesetz vom 03.05.2013 (BGBl. I S. 1084), zuletzt geändert durch Gesetz vom 18.07.2017 (BGBl. I S. 2745)
BWahlG	Bundeswahlgesetz i. d. F. der Bekanntmachung vom 23.07.1993 (BGBl. I S. 1288, 1594), zuletzt geändert durch Gesetz vom 08.06.2017 (BGBl. I S. 1570)
DSAnpUG-EU	Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30.06.2017 (BGBl. I S. 2097)
DS-GVO	Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), (ABl. EU L 119, S. 1)
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche i. d. F. vom 21.09.1994 (BGBl. I S. 2494; 1997 I S. 1061), zuletzt geändert durch Gesetz vom 20.07.2017 (BGBl. I S. 2787)
GemHVO	Verordnung über die Aufstellung und Ausführung des Haushaltsplans der Gemeinden (Gemeindehaushaltsverordnung) GVBl. II 331-27 vom 02.04.2006 (GVBl. I S. 235), zuletzt geändert durch Verordnung vom 07.12.2016 (GVBl. S. 254)
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23.05.1949 in der im BGBl. III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 13.07.2017 (BGBl. I S. 2347)
GlüStV	Staatsvertrag zum Glücksspielwesen in Deutschland (Glücksspielstaatsvertrag) vom 15.12.2011 (GVBl. 2012 S. 190, 197), in Kraft getreten am 01.07.2012 gemäß Bekanntmachung vom 10.08.2012 (GVBl. S. 264)
HArchivG	Hessisches Archivgesetz vom 26.11.2012 (GVBl. S. 458)
HGlüG	Hessisches Glücksspielgesetz vom 28.06.2012 (GVBl. S. 190)
HGO	Hessische Gemeindeordnung i. d. F. vom 07.03.2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 15.09.2016 (GVBl. I S. 167)

HGO	Hessische Gemeindeordnung i. d. F. der Bekanntmachung vom 07.03.2005 (GVBl. I S. 142), zuletzt geändert durch Gesetz vom 15.09.2016 (GVBl. S. 167)
HMG	Hessisches Meldegesetz i. d. F. vom 10.03.2006 (GVBl. I S. 66), zuletzt geändert durch Gesetz vom 28.09.2015 (GVBl. S. 346)
KAG	Gesetz über kommunale Abgaben (GVBl. II 334-7) i. d. F. vom 24.03.2013 (GVBl. S. 134), zuletzt geändert durch Gesetz vom 20.12.2015 (GVBl. S. 618)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie vom 09.01.1907 in der im BGBl. III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Gesetz vom 16.02.2001 (BGBl. I S. 266)
KWG	Hessisches Kommunalwahlgesetz i. d. F. der Bekanntmachung vom 07.03.2005 (GVBl. I S. 197), zuletzt geändert durch Gesetz vom 20.12.2015 (GVBl. S. 618)
LuftVG	Luftverkehrsgesetz i. d. F. vom 10.05.2007 (BGBl. I S. 698), zuletzt geändert durch Gesetz vom 20.07.2017 (BGBl. I S. 2808)
LuftVO	Luftverkehrs-Ordnung vom 29.10.2015 (BGBl. I S. 1894), zuletzt geändert durch Verordnung vom 11.06.2017 (BGBl. I S. 1617)
LuftVZO	Luftverkehrs-Zulassungs-Ordnung vom 19.06.1964 (BGBl. I S. 370), zuletzt geändert durch Verordnung vom 30.03.2017 (BGBl. I S. 683)
LWG	Gesetz über die Wahlen zum Landtag des Landes Hessen (Landtagswahlgesetz) i. d. F. der Bekanntmachung vom 07.04.2006 (GVBl. I S. 110, 439), zuletzt geändert durch Gesetz vom 18.12.2017 (GVBl. S. 478)
OWiG	Gesetz über Ordnungswidrigkeiten i. d. F. vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 27.08.2017 (BGBl. I S. 3295)
PaßG	Paßgesetz vom 19.04.1986 (BGBl. I S. 537), zuletzt geändert durch Gesetz vom 07.07.2017 (BGBl. I S. 2310)
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) vom 18.06.2009 (BGBl. I S. 1346), zuletzt geändert durch Gesetz vom 18.07.2017 (BGBl. I S. 2745)
RED-G	Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus vom 20.08.2012 (BGBl. I S. 1798), zuletzt geändert durch Gesetz am 14.08.2017 (BGBl. I S. 3202)
SchfHwG	Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk (Schornsteinfeger-Handwerksgesetz) vom 26.11.2008 (BGBl. I S. 2242), zuletzt geändert durch Gesetz vom 17.07.2017 (BGBl. I S. 2495)
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil – i. d. F. vom 11.12.1975 (BGBl. I S. 3214, 3219), zuletzt geändert durch Gesetz vom 17.08.2017 (BGBl. I S. 3214, 3219)
SGB II	Sozialgesetzbuch Zweites Buch – Grundsicherung für Arbeitsuchende – i. d. F. vom 13.05.2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Gesetz vom 17.07.2017 (BGBl. I S. 2541, 2556)
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung – i. d. F. vom 20.12.1988 (BGBl. I S. 2477, 2482), 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 30.10.2017 (BGBl. I S. 3618)

SGB XII	Sozialgesetzbuch Zwölftes Buch – Sozialhilfe – i. d. F. vom 27.12.2003 (BGBl. I S. 3022, 3023), zuletzt geändert durch Gesetz vom 17.08.2017 (BGBl. I S. 3214, 3217)
StGB	Strafgesetzbuch i. d. F. vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618)
StPO	Strafprozessordnung i. d. F. vom 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618)
StVG	Straßenverkehrsgesetz i. d. F. vom 05.03.2003 (BGBl. I S. 310, 919) zuletzt geändert durch Gesetz vom 17.08.2017 (BGBl. I S. 3202)
TMG	Telemediengesetz vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Gesetz vom 28.09.2017 (BGBl. I S. 3530)
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)
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 09.09.1965 (BGBl. I S. 1273), zuletzt geändert durch Gesetz vom 01.09.2017 (BGBl. I S. 3346)
UWG	Gesetz gegen den unlauteren Wettbewerb i. d. F. vom 03.03.2010 (BGBl. I S. 254, zuletzt geändert durch Gesetz vom 17.02.2016 (BGBl. I S. 233)

Kernpunkte

1. Die Vorbereitungen auf die neue Rechtslage nach Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) waren im Berichtsjahr vordringliches Thema. Verantwortliche, behördliche und betriebliche Datenschutzbeauftragte müssen sich auf Änderungen einstellen (z. B. Ziff. 2.3, Ziff. 2.4). Die Aufsichtsbehörden haben für eine erste Orientierung gemeinsam Kurzpapiere zu verschiedenen Themen der DS-GVO erarbeitet und veröffentlicht (Ziff. 19).

2. Auf EU-Ebene wird eine IT-Infrastruktur bereitgestellt werden, die die kooperativen Verfahren und das Kohärenzverfahren nach DS-GVO ermöglichen wird. In der zuständigen EU-Arbeitsgruppe, der IT Task Force, vertritt Hessen die Interessen aller Landesdatenschutzbehörden Deutschlands (Ziff. 4.2).

3. Die erste Überprüfung des Privacy Shield hat stattgefunden. Es besteht datenschutzrechtlicher Nachbesserungsbedarf (Ziff. 4.1).

4. Fragen zu den Rahmenbedingungen möglicher Auftragsdatenverarbeitung und Outsourcing im öffentlichen und nichtöffentlichen Bereich werden in den Beiträgen Ziff. 5.1 (Verkehrsüberwachung), Ziff. 7.4 (Gesundheitsbereich), Ziff. 8.5 (Sozialbereich) und Ziff. 15.4 (Übertragung hoheitlicher Aufgaben) behandelt.

5. Im Gesundheitsbereich kommt es immer wieder zu Datenschutzverstößen, die wegen der Sensibilität der betroffenen Patientendaten besonders ärgerlich sind. Betroffen sind Kliniken (Ziff. 7.1, 7.3) ebenso, wie z. B. die Terminverwaltung in Arztpraxen (Ziff. 7.5). In einem klinischen Forschungsprojekt konnte ich dagegen vorab beratend die richtigen datenschutzrechtlichen Weichen stellen (Ziff. 7.2), gleiches galt bei einem beabsichtigten Forschungsvorhaben mit Adoptionsvermittlungsakten (Ziff. 8.4).

6. Foto- und Videoaufnahmen sind nach wie vor Anlass zu Beschwerden. Bei diesem Thema werden die Schutzbereiche des Rechts auf informationelle Selbstbestimmung besonders deutlich. Betroffen sind nahezu alle Lebensbereiche: Kindertagesstätten (Ziff. 8.2), Schulen (Ziff. 9.5), öffentlich zugängliche Bereiche (Ziff. 11.3) und Verkehr (Ziff. 15.2).

7. Die Digitalisierungswelle hat den Schulbereich erreicht:
   Mit der frühzeitigen Einbindung der Aufsichtsbehörden in das Projekt „Digitales Lernen unterwegs“ kann ein anspruchsvolles Projekt im Bereich schulischer Betreuung von Kindern beruflich Reisender realisiert werden (Ziff. 9.2).

Der Einsatz von Microsoft Office 365 an hessischen Schulen ist datenschutzrechtlich möglich (Ziff. 9.3).

8. Die Hessenbox unterstützt mit einer Cloud-Speicherlösung den Austausch von Dokumenten an hessischen Hochschulen (Ziff. 16.1).

9. Das Kopieren von Personalausweisen zum Abgleich und Feststellung von Identitäten geht schnell, ist verbreitet, aber nicht immer zulässig. Datenschutzrechtliche Bewertungen erfolgen zur neuen Gesetzeslage (Ziff. 3.1) sowie zu typischen Beschwerdefällen (Ziff. 11.1, Ziff. 13.2).

10. Die Wirtschaft erhebt personenbezogene Daten von Kunden und Verbrauchern – absichtlich oder unabsichtlich – nicht immer in zulässiger Weise; so z. B. bei der Aufzeichnung von Gesprächsinhalten am Telefon (Ziff. 11.2), der Freischaltung eines DVB-T-Empfängers (Ziff. 11.5), bei der Buchung eines Ferienhauses (Ziff. 12.2). Allerdings verschiebt sich auch die gängige Erwartungshaltung von Kunden: Die Übermittlung von E-Mail-Adressen eines Kunden durch den Händler an Postdienstleister zu Zustellzwecken ist nicht unzulässig (Ziff. 12.1).

11. Technische Maßnahmen sind für einen ausreichenden Datenschutz existentiell und stehen zunehmend im Fokus einer datenschutzrechtlichen Prüfung (Ziff. 12.3, Ziff. 16.2).

1. Einführung

1.1
Allgemeines

1.1.1
Anknüpfung an den 45. Tätigkeitsbericht

In der Einführung zum 45. Tätigkeitsbericht (TB) wurde die Entstehung des Datenschutzes in den 1970er Jahren und die Herleitung der Datenschutzgrundrechte als Unterfall der informationellen Selbstbestimmung in groben Zügen dargestellt. Daran knüpfte ein Überblick über die derzeitige Gefährdungslage der informationellen Selbstbestimmung an. „Datenschutz“ wurde dabei im Sinne eines Synonyms für „informationelle Selbstbestimmung“ als enger (Rechts-) Begriff verwendet: „Datenschutz“ war Personenschutz im Gegensatz zum weiteren allgemeinen Wortverständnis, wonach „Datenschutz“ den Schutz der Daten selbst meint. Die jüngste Rechtsentwicklung lässt Ansätze zur Erweiterung des Rechtsbegriffs erkennen. Insoweit ist der 45. TB nicht mehr ganz aktuell. Die Realanalyse im 45. TB wurde dagegen durch die aktuelle Entwicklung in vollem Umfang bestätigt. Die nachfolgenden allgemeinen Bemerkungen dienen zur Vertiefung, Ergänzung und Fortführung der allgemeinen Bemerkungen in den früheren Berichten.

1.1.2
Daten

Der Datenschutz setzt ein Verständnis von Daten voraus, das bis in die Frühzeit der Menschheit zurückreicht. Der Mensch musste seine defizitäre Ausstattung als Instinktwesen durch geistige Leistungen ausgleichen. Das erforderte die Fähigkeit, auf die Umweltbedingungen zu reagieren, sie wahrzunehmen und in ihrer Tragweite zu erfassen. Dadurch entstand Wissen, das „in Form“ gebracht werden musste, damit es bei Bedarf abgerufen werden kann. Geformt wird Wissen, indem es in begreifbare Teilmengen zerlegt wird. Die Teilmengen sind *Informationen*. Solche Informationen werden gesammelt, erfasst und gespeichert und können dann den Mitmenschen mitgeteilt werden. Mitteilungen sind nötig, weil der Mensch nur in Gemeinschaft existieren kann. Zur Verarbeitung und Übermittlung an Dritte werden die Informationen zu *Daten*. Daten sind ihrem lateinischen Wortsinn nach „An-Gaben“. Im wechselseitigen Datenaustausch entwickelte sich das, was man seit dem 16. Jahrhundert „Kommunikation“ nennt.

Im 21. Jahrhundert bezeichnet Kommunikation den „Informationsaustausch“. Durch die Kommunikation werden die Informationen nicht nur verknüpft, sondern auch im Wechselspiel vermehrt. Im Rahmen der Informationsverarbeitung entstehen noch nicht informationell verarbeitete Rohdaten; mit der Verarbeitung dieser Daten wird ein informationeller Mehrwert (*Informationsmehrwert)* erzeugt. Ein Mehrwert entsteht aber auch bereits durch die Möglichkeiten, organisatorisch mit Datenmengen umzugehen, Daten zu verarbeiten und zu übermitteln (*Verarbeitungsmehrwert*). Die manuelle Datenverarbeitung zum Zweck des Informationsaustauschs gab es schon in der Antike. Die zusätzlich zum Wert einer Information als solcher entstehenden Wertkategorien erlangten jedoch erst mit der maschinellen und elektronischen Datenverarbeitung Relevanz. Mit der Automatisierung der Datenverarbeitung verlagerte sich das Augenmerk von den Daten auf die Informationen. Sprachlich wurde häufig nicht mehr zwischen Informationen und Daten unterschieden. Das gilt insbesondere für den juristischen Sprachgebrauch. Daten sind danach maschinenlesbare Informationen. Rechtlich bedeutsam ist in erster Linie der Informationsgehalt der Daten. Speziellen Informationsgehalt haben dabei Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (*personenbezogene Daten*). Von diesen Informationen kann die betroffene Person selbst Gebrauch machen. Sie sind aber auch Dritten zugänglich. Die Möglichkeit, automatisiert Daten zu verarbeiten, umfasst die Möglichkeit, sich Informationen über dritte Personen zu verschaffen, die diese Daten nicht preisgeben wollen. So entsteht einerseits ein *Datenverkehr*, bei dem durch die automatisierte Datenverarbeitung ein gesamtgesellschaftlich erheblicher, nicht zuletzt wirtschaftlicher Wert erzeugt wird. Der Datenverkehr greift andererseits massiv in die Rechtsstellung Betroffener ein. Datenschutz und Datenverkehr werden daher zumeist als *Gegensätze* behandelt und betrachtet. So führt laut *Ziebarth* (in: Sydow, Europäische Datenschutzgrundverordnung, Komm., 2017, Art. 51 Rdnr. 18 ff.) Art. 51 Abs. 1 DS-GVO zwar zwei Gründe für die Errichtung von Aufsichtsbehörden an, nämlich den Grundrechtsschutz bei der Verarbeitung personenbezogener Daten und die Erleichterung des Datenverkehrs. Die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung zu schützen, sei aber der unmittelbare und eigentliche Zweck der Aufsichtsbehörden. Die Aufsichtsbehörden dienten dagegen nicht unmittelbar der Förderung des freien Datenverkehrs. Dies dürfte dem Selbstverständnis der meisten Aufsichtsbehörden entsprechen (vgl. *Körffer*, in Paal/Pauly, Datenschutz-Grundverordnung, Komm., 2017, Art. 51 Rdnr. 6). Demgegenüber geht Erwägungsgrund 123 der DS-GVO ersichtlich von einer doppelten Zielsetzung aus. In diesem Sinne spricht *Selmayr* (in: Ehmann/Selmayr, Datenschutz-Grundverordnung, Komm., 2017, Art. 51 Rdnr. 3) von einer doppelten Aufgabe der Aufsichtsbehörden. Das ändert jedoch nichts an der Annahme konträrer Ziele, die „miteinander ins Gleichgewicht“ zu bringen sind (EuGH, ECLI:EU:C:2014:237 – Kommission/Ungarn).

1.1.3
Schutz personenbezogener Daten

Durch die Möglichkeiten der automatisierten Datenverarbeitung entsteht die Gefahr, dass Betroffene durch den Fremd-Umgang mit ihren Daten in ihren Rechten verletzt werden. Dem zu begegnen, wurde der Datenschutz, weltweit erstmalig, in Hessen in einem Datenschutzgesetz (Hessisches Datenschutzgesetz vom 07.10.1970 (GVBl. I S. 31; hierzu bereits der 1. TB des HDSB, LTDrucks. 7/1495) entwickelt. Es ging dabei, wie erwähnt, nicht um den Schutz der Daten *als solcher*, sondern um den Schutz der hinter den Daten stehenden Person, d. h. um das *allgemeine Persönlichkeitsrecht*. Das *allgemeine* Persönlichkeitsrecht hatte sich in der deutschen Rechtsordnung nur allmählich durchgesetzt. So führten die Verfasser des BGB in § 823 Abs. 1 lediglich *einzelne* Persönlichkeitsgüter auf. Das Reichsgericht lehnte noch die Annahme und *Kommerzialisierung* eines allgemeinen Persönlichkeitsrechts ab (RGZ 113, 413), das dann aber vom BGH in seiner frühen Rechtsprechung bejaht und einschließlich eines Geldentschädigungsanspruchs in Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG verortet wurde (BGHZ 13, 334). Dies fand die Billigung des Bundesverfassungsgerichts im Soraya-Beschluss vom 14.02.1973 (BVerfGE 34, 269). Schon vorher hatte das Bundesverfassungsgericht ein Grundrecht auf Privatheit anerkannt: In der Mikrozensus-Entscheidung vom 16.07.1969 (BVerfGE 271, 1) hatte es ausgeführt, dass dem Staat ein Eindringen in den Persönlichkeitsbereich durch eine umfassende Einsichtnahme in die persönlichen Verhältnisse seiner Bürger versagt sei. Diese Rechtsprechung zog das Bundesverfassungsgericht nunmehr zur Begründung eines zunächst nur defensiv gedachten Datenschutzgrundrechts heran. Durch das im Volkzählungsurteil (BVerfGE 65, 1) kreierte Grundrecht der informationellen Selbstbestimmung schuf es jedoch die Voraussetzungen für ein weiter gefasstes personales Datenschutzverständnis. Das Recht auf informationelle Selbstbestimmung gewährleistete die „Befugnis der Person, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ dürfen und beinhaltete damit das *autonome* Verfügungsrecht der Betroffenen über ihre persönlichen Daten. Durch die Kombination mit Art. 2 Abs. 1 GG wurde das Abwägungsverbot des Art. 1 Abs. 1 GG aufgehoben. Das Grundrecht auf informationelle Selbstbestimmung ist der Einschränkung im überwiegenden Interesse der Allgemeinheit oder Dritter zugänglich. Die Belange des Datenschutzes sind im jeweiligen Sachzusammenhang mit konträren Belangen der Allgemeinheit oder Einzelner abzuwägen. Das Recht auf informationelle Selbstbestimmung gewährt demzufolge „kein unbeschränktes dingliches Herrschaftsrecht über bestimmte Informationen, sondern findet seine Grenzen in den Rechten Dritter, insbesondere der Informations-, Meinungs- und Medienfreiheit.“ An diesem Datenschutzverständnis, das auch in das Bundesdatenschutzgesetz vom 01.02.1977 (BGBl. I S. 201) einging, hielt das Bundesverfassungsgericht noch im

Berichtzeitraum fest (BVerfG, NJW 2017, 466). Mittlerweile hat sich aber der Schutzcharakter der informationellen Selbstbestimmung verändert. Der Staat hat die informationelle Selbstbestimmung nicht nur zu achten; er hat sie auch zu schützen. Diese Verpflichtung trifft alle Staatsorgane. Neben der Abwehr hoheitlicher Eingriffe entwickelte sich der Anspruch auf staatliches Einschreiten gegen Datenschutzverstöße privater Dritter. Über den Schutzanspruch erlangten die Datenschutzgrundrechte mittelbare Drittwirkung. Hinzu kam die Aufgabe des Staates, die informationelle Selbstbestimmung generell durch die Vorsorge für eine erforderliche Infrastruktur zu gewährleisten. Das grundrechtskonforme Funktionieren der elektronischen Netze ist im Digitalisierungszeitalter eine Aufgabe der *Daseinsvorsorge*. Das Recht auf informationelle Selbstbestimmung gewährleistete somit generell die „Befugnis der Person, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“ Zur weiteren Entwicklung wird auf die nach wie vor gültigen Ausführungen im 45. TB verwiesen:

“Geschützt wird nicht lediglich und nicht einmal primär die Privatsphäre vor invasiven Eingriffen. Geschützt wird der ungehinderte Informationsaustausch. Der heutige Mensch will informativ und kommunikativ mit anderen in Verbindung treten. Er will Informationen verbreiten und möglichst umfassend und korrekt über alles und jedes informiert werden, aber autonom bestimmen, welche ihn betreffende Informationen verarbeitet werden und in die Öffentlichkeit gelangen dürfen. Informationszugangsfreiheit und Datenschutz sind zwei Seiten der gleichen Medaille. Ein richtig verstandenes Datenschutzgesetz ist immer zugleich ein Informationsfreiheitsgesetz. Hinzu kommt die Datensicherheit, die noch am ehesten dem Datenschutz als solchem nahekommt, aber ebenfalls einen personalen Schutzzweck verfolgt. Für die informationelle Selbstbestimmung ist die Sicherheit der Daten unverzichtbar. Datenschutz, Informationszugangsfreiheit und Informationssicherheit gehören zusammen. Ihre Kombination generiert die individuelle Datenhoheit oder Datensouveränität. Der Staat hat die informationelle Selbstbestimmung nicht nur zu achten; er hat sie auch zu schützen. Diese Verpflichtung trifft alle Staatsorgane. Die Intensität des Schutzes hängt vom Grad der Gefährdung der informationellen Selbstbestimmung ab. Vor allem durch das Fortschreiten der Digitalisierung hat die Gefährdung eine Dimension erreicht, die Zweifel weckt, ob ein zureichender Schutz der informationellen Selbstbestimmung überhaupt noch gewährleistet werden kann.“

Die irreführend als Datensouveränität bezeichnete (Souveränität bedeutet als Begriff der Allgemeinen Staatslehre das Monopol legitimer Gewaltausübung; übertragen auf die Hoheitsbefugnisse Privater, würde deren Datensouveränität zu einem absoluten Verbot der Verarbeitung ihrer Daten durch Dritte führen) *Datenhoheit* wirkt zwar gegen jedermann, sie ist aber kein umfassendes absolutes Recht, sondern kollidiert mit Rechten Dritter, die sich ebenfalls auf

Freiheitsrechte berufen können. Freiheitsgebrauch ist auch die Sammlung, Erhebung, Verarbeitung und Weitergabe personenbezogener Daten von Dritten. Die Abwägung der jeweiligen Rechtspositionen setzt voraus, dass Klarheit über die Ausprägungen der Datenhoheit herrscht. Element der Datenhoheit ist die Kontrolle über die eigenen Daten als Ausdrucksform des allgemeinen Persönlichkeitsrechts. Das ist mit der Bezeichnung „Datenautonomie“ gemeint. Das Persönlichkeitsrecht ist auf „Entfaltung“ der Persönlichkeit angelegt. Persönlichkeit entfaltet sich in der Gesellschaft in der Kommunikation und Interaktion und in der Beteiligung am Wirtschaftsleben. Das rechtfertigt die Berücksichtigung kommerzieller Aspekte bei der Bestimmung des Persönlichkeitsrechts, die auch bei der informationellen Selbstbestimmung geboten ist. Datenschutz und Datenverkehr sind somit *nicht* notwendig Gegensätze.

1.1.4
Datenverkehr und Datenhandel

Wird der Datenverkehr nicht nur als Beschränkung, sondern auch als Erscheinungsform des Datenschutzes angesehen, dann müssen sich die neuesten Entwicklungen des Datenverkehrs unmittelbar auf die Ausgestaltung des Datenschutzes auswirken. Vor allem als Folge der Digitalisierung ändern sich in nahezu allen Lebensbereichen die politischen Akzente und rechtlichen Bewertungen (vgl. *Hengstenberg*, NJW 2017, 433). So ist eine Datenverarbeitung möglich geworden, die niemand auch nur erahnen konnte, als man die ersten datenschutzrechtlichen Regelungen traf. Mittlerweile ist die Ära des allgegenwärtigen Rechnens („Ubiquitous Computing“) angebrochen, bei der die zahlreichen wirtschaftlichen und sozialen Chancen der digital vernetzten Computersysteme das Risiko des Kontrollverlusts über die eigenen Daten in den Hintergrund treten lassen. Die wirtschaftliche Verwertung jeglicher Daten wurde zum alles beherrschenden Thema. Der Datenhandel als Erscheinungsform des Datenverkehrs hat dem Datenschutz den Rang abgelaufen. Strategisches Ziel der EU-Kommission ist es, den Datenhandel insgesamt zu erweitern. Wohl eher aus taktischen Gründen wird der Handel mit personenbezogenen Daten (zunächst) ausgeklammert (vgl. die Mitteilung „Building an European Data Economy“ vom 10.01.2017 k COM (2017) 2 final; hierzu Staff working document, COM (2017) 9 final.). Unter Big Data-Bedingungen wird jedoch die Fortentwicklung der „Data Economy“ bei den nicht personenbezogenen Daten die personenbezogenen Daten und damit den Datenschutz nicht unberührt lassen. Big Data bedeutet die Verknüpfung einer derartigen Vielzahl von Daten, dass die herkömmlichen die Datenschutzprinzipien als Anachronismen erscheinen (*Boehme-Neßler*, DuD 2016, 419 ff.; *Sarunski*, DuD 2016, 424 ff.; *Marnau*, DuD 2016, 428 ff.; *Steinebach/Krempel/Jung/Hoffmann*, DuD 2016, 440 ff.; auch *Karl-Heinz Ladeur*, DuD 2016, 360 ff.; *Katrin Schaar*, ZD 2016, 224 ff.). Manche meinen, wir

müssten uns auf die Epoche ohne Privatsphäre (post privacy) einstellen. Umgekehrt kann man argumentieren, dass Big Data durch die Verknüpfungsmöglichkeiten alle Daten zu personenbezogenen Daten mache, was zu einer immensen Ausdehnung des Datenschutzrechts führen würde. Die Entwicklung vom Datenschutz als Personenschutz zum Datenschutz als Schutz der Daten selbst zeichnet sich deutlich ab. Das vieldiskutierte Dateneigentum verlangt nach einer Zuordnung des Informations- und Verarbeitungsmehrwerts. Die informationelle Selbstbestimmung könnte dann auf Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1, Art. 12 Abs. 1 und Art. 14 Abs. 1 GG gestützt werden. Diese Problematik wird freilich erst in Zukunft zu bewältigen sein. Bereits jetzt stellt sich jedoch die Frage nach einer Neubestimmung des Verhältnisses von Datenschutz und Datenhandel. Diese ist im gegenwärtig diskutierten „neuen“ Datenschutzrecht aber noch nicht vorgenommen.

1.2.
Das neue Datenschutzrecht

1.2.1
Überblick

Das Datenschutzrecht befindet sich in permanentem Umbruch. Die Datenverarbeitungstechnik entwickelt sich so schnell, dass die supranationalen und nationalen rechtlichen Regelungen kaum Schritt halten können. Auch die gegenwärtig stattfindende, grundlegende europäische Datenschutzreform stellt nur einen Teilschritt in der Fortentwicklung des Datenschutzrechts dar. Gleichwohl wurden die Datenschutzaktivitäten der Aufsichtsbehörden im Berichtszeitraum schwerpunktmäßig durch die Vorbereitung auf das künftig in weiten Teilen unmittelbar geltende Datenschutzrecht der EU bestimmt. Über die Entstehung und Bedeutung der Verordnung (EU) 2016/679 (DS-GVO) und der Richtlinie (EU) 2016/680 (DS-RL), die am 25.05.2016, also vor dem Berichtzeitraum, in Kraft traten (Art. 99 Abs. 1 DS- GVO; Art. 64 DS-RL), wurde in den vorangegangenen TB berichtet. Die DS-GVO wird erst am 25.05.2018, also in dem diesem TB folgenden Berichtszeitraum Geltung erlangen (Art. 99 Abs. 2 DS-GVO). Auch die DS-RL ist erst bis zum 06.05.2018 umzusetzen (Art. 65 Abs. 1 DS-RL). Für den vorliegenden Berichtszeitraum ist somit inhaltlich nur im Rahmen von Einzelfragen auf die unionsrechtlichen Regelungen einzugehen. Für die Mitarbeiterinnen und Mitarbeiter des HDSB kam es in erster Linie darauf an, insbesondere die unmittelbare Geltung der DS-GVO vorzubereiten und eventuelle Vorwirkungen zu berücksichtigen. Der Bundesgesetzgeber und die Landesgesetzgeber waren aufgerufen, die erforderlichen Umsetzungs- und Konkretisierungs-

regelungen und in Bereichen fehlender Unionszuständigkeit originäre, aber gleichwohl kohärente Regelungen zu treffen. Der Bund brachte dies durch den Oberbegriff „Anpassungsgesetz“ zum Ausdruck. In Hessen befindet sich eine zeitgemäße umfassende Normierung der informationellen Selbstbestimmung in der Beratung. In die den Bund und das Land Hessen betreffenden Gesetzgebungsverfahren war der HDSB etwa in Form von „Kontaktrunden“ eingebunden.

1.2.2
DS-GVO

Die Vorwirkungen der DS-GVO sind ggf. bei den einzelnen Berichtspunkten berücksichtigt.

1.2.3
BDSG

Das Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 60) wurde durch Art. 8 Abs. 1 Satz 2 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) vom 30.06.2017 (BGBl. I S. 2097) ersetzt. Das Artikelgesetz enthält eine, die unionsrechtlichen Vorgaben konkretisierende und ergänzende, umfassende Neuregelung des allgemeinen Datenschutzrechts für öffentliche Stellen des Bundes und der Länder sowie für nicht öffentliche Stellen (vgl. BTDrucks. 18/11320;18/2084). In dem gleichen Artikelgesetz erfolgten Folgeänderungen im Bundesverfassungsschutzgesetz, MAD-Gesetz, BND-Gesetz, Sicherheitsüberprüfungsgesetz und Artikel 10-Gesetz. Der Geltungsbeginn des Gesetzes ist auf den 25.05.2018 datiert. Das neugefasste Bundesdatenschutzgesetz besteht aus vier Teilen. Teil 1 enthält allgemeine Bestimmungen und Teil 2 Durchführungsbestimmungen zur Datenschutz-Grundverordnung. Teil 3 führt die Datenschutz-Richtlinie aus. Teil 4 betrifft die Regelung der Datenverarbeitung im originären Zuständigkeitsbereich des Bundesgesetzgebers.

Über inhaltliche Probleme ist für den Berichtszeitraum noch nichts zu berichten.

1.2.4
Hessisches Informationsfreiheitsgesetz

Im Berichtszeitraum wurde der Referentenentwurf 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 nach dem Stand vom 28.08.2017 vorgelegt. In die Arbeiten am Entwurf war der HDSB ständig eingebunden. Daraus entstand die Vorlage vom 05.12.2017 (LTDrucks. 19/5728), die inhaltlich im Berichtszeitraum nicht mehr gewürdigt werden konnte.

1.3
Aktivitäten des HDSB zur Umsetzung DS-GVO

Kursorischer Überblick zum Stand der inhaltlichen Umsetzung des Datenschutzreformpakets beim/durch HDSB

Die europäische Datenschutzreform hat bei nahezu allen öffentlichen und nicht öffentlichen Stellen im Berichtsjahr außerordentlichen Umsetzungsbedarf ausgelöst, nicht zuletzt in meiner Behörde. Neben den übergreifenden „Großprojekten“, die im Zusammenwirken der nationalen und europäischen Datenschutzbehörden untereinander zu bewältigen sind, sind auch zahlreiche innerorganisatorische Anpassungen und Neuerungen vorzunehmen. Dies führte zu einem erheblichen Mehraufwand für die Mitarbeiterinnen und Mitarbeiter meiner Dienststelle, der mit den vorhandenen Ressourcen zu bewältigen war.

Hier einige Beispiele:

– Die in 2016 bereits begonnene hausinterne Grundsatzschulung zur Datenschutzgrund-Verordnung (erste Stufe im Vortragsformat) wurde im ersten Halbjahr 2017 abgeschlossen.

– Zur Konkretisierung der Umsetzungsbedarfe und der Erarbeitung von Lösungen wurden in einer zweiten Stufe hausinterne Projektgruppen gebildet. Diese haben sich mit einzelnen, für die Umsetzung relevanten, Fragestellungen intensiv auseinandergesetzt und werden teilweise auch noch über 2017 hinaus damit befasst sein. Insgesamt waren über 60 Fragestellungen in verschiedensten Fallvarianten herausgearbeitet worden und zu beantworten.

– Die Fragestellungen mündeten (in dritter Stufe) in die Erarbeitung praktischer behördeninterner Umsetzungsvorschläge, die bereits in Angriff genommen und teilweise auch schon abgeschlossen sind, wie z. B. Anpassung der Behördenorganisation an die neue Bedarfslage, Ausbau der englischen Sprachkenntnisse, Aufbau einer neuen Homepage, Anpassung der Aktenführung, Überarbeitung von Meldeformularen, Aufbau eines Fristenkalenders, Aufbau eines Justiziariats mit Sanktionsstelle, Erweiterung des bestehenden Testlabors zu einem leistungsfähigeren IT-Laboratorium, Überblick über technische Erforderlichkeiten bzgl. sicherer Kommunikation etc.

– Gleiches gilt für die Erarbeitung praktischer Umsetzungsvorschläge für neue Aufgaben mit Außenkontakten wie z. B. Organisation der zentralen Anlaufstelle und die Organisation der Datenschutzaufsichtsbehörden in Deutschland mit Blick auf die Gewährleistung eines funktionierenden Kohärenzverfahrens vor dem Europäischen Datenschutzausschuss.

– Erheblichen Aufwand verursachte und verursacht noch die rechtliche Aufarbeitung strittiger Fragen bei der Auslegung der DS-GVO, die letztlich in den bisher veröffentlichten gemeinsamen Kurzpapieren der DSK und weiteren Empfehlungen bzw. Informationsmaterialien (siehe z. B. Ziff. 19 sowie auf meiner Homepage www.datenschutz.hessen.de) ihren Niederschlag fanden sowie in ersten Veröffentlichungen in Zeitschriften zum Beispiel zum Thema Sanktionen (Rost, RDV 2017, 13).

– Weiterhin war meine Behörde intensiv in die Erstellung eines Entwurfs zum HDSG-neu eingebunden und es fanden intensive Beratungen der mit der Anpassung der Landesgesetzgebung befassten Behörden statt.

– Die Anzahl der Sitzungen der Arbeitsgruppen, Arbeitskreise und Konferenzen der Aufsichtsbehörden auf Landes-, Bundes- und europäischer Ebene zu spezifischen Fachthemen und zur Klärung von Umsetzungsfragen war deutlich gestiegen.

  Zu behandelnde Themen waren unter anderem die Zentrale Anlaufstelle (ZASt), die Geschäftsordnung der Datenschutzkonferenz, Akkreditierung durch die DAkkS, Konformitätsbewertungsprogramme, Homepage DSK, Anpassung der Landesdatenschutzgesetze, Meldeformulare nach DS-GVO, Codes of Conduct, Erstellen von ersten Informationsblättern und die IT-technische Umsetzung des Kohärenzverfahrens nach Art. 63 - 67 DS-GVO.

– Darüber hinaus haben meine Mitarbeiterinnen und Mitarbeiter und ich mit Vorträgen und Schulungen verschiedenste verantwortliche Stellen der Datenverarbeitung und Interessierte aus dem öffentlichen und nichtöffentlichen Bereich über die anstehende Reform informiert.

Die Datenschutzreform wird ab 25.05.2018 Geltung erlangen. Bis dahin werden noch zahlreiche Aufgaben und Herausforderungen auf nationaler und europäischer Ebene zu bewältigen sein. Ich sehe meine Behörde – und auch die übrigen Aufsichtsbehörden – auf einem guten Weg, bis zu diesem Zeitpunkt die europäischen Vorgaben zu erfüllen.

1.4
Arbeitsstatistik 2017

1.4.1
Eingaben und Beratungen

Im Berichtsjahr hat sich insbesondere die Anzahl der telefonischen Beratungen im Vergleich zum Vorjahr deutlich erhöht. Diese Steigerung war auf zahlreiche Nachfragen von Unternehmen und betrieblichen Datenschutzbeauftragten zu einzelnen Themen der bevorstehenden Änderungen durch die EU-Datenschutzreform und die Neuregelung des Bundesdatenschutzgesetzes zurück zu führen.

In der nachfolgenden Tabelle sind Angaben zur Anzahl der Eingaben und Beratungsanfragen dargestellt, die neben der Bearbeitung von Grundsatzfragen, Stellungnahmen zu Gesetzesvorhaben und der Marktbeobachtung im Bereich von IT-Produkten einen wesentlichen Teil meiner Tätigkeit ausmachen. Diese Statistik wird weitgehend automationsgestützt mit Hilfe des eingesetzten Dokumentenverwaltungssystems erstellt. Nicht erfasst werden dort die zahlreichen telefonisch eingegangenen und telefonisch erledigten Eingaben und Beratungen, die zwar keinen Niederschlag in Akten gefunden haben, aber oft einen erheblichen Zeitaufwand verursachen. Die telefonischen Eingaben und Beratungen wurden für den Monat November als Stichprobe gezählt und für das Jahr hochgerechnet.

Die Anzahl der schriftlich dokumentierten Beratungen und Eingaben ist leicht gestiegen. Erneut liegt der Schwerpunkt im Bereich „Miete, Wohnen, Nachbarschaft“ mit zahlreichen Eingaben zur Videobeobachtung durch Haus- und Wohnungseigentümer bzw. Nachbarn. Auffäl-

lig mehr Eingaben bzw. Beratungen als im Vorjahr waren in den Bereichen „Schulen und Hochschulen“, „Beschäftigtendatenschutz“ sowie „IT-Sicherheit, DV-Technik und Herstelleranfragen“ zu verzeichnen. Erstmals gab es zudem nennenswerte übernationale Nachfragen (Europa bzw. International), was zum einen ebenfalls auf die EU-Datenschutzreform, aber auch auf Vorgänge um internationale Datentransfers zurückzuführen war.

Die Mengenübersicht der Eingaben und Beratungen stellt sich wie folgt dar:

Fachgebiet	**Anzahl 2017**
Wohnen, Miete, Nachbarschaft	328
Auskunfteien und Inkassounternehmen	205
Schulen, Hochschulen, Archive	189
Elektronische Kommunikation, Internet	168
Beschäftigtendatenschutz (Personalwesen)	163
Kommunen	148
Adresshandel, Werbung	130
Gesundheit, Pflege	112
Kreditwirtschaft	102
Soziales	95
Polizei, Strafverfahren, Justiz , Verfassungsschutz	92
Verkehr	71
Handel, Handwerk, Gewerbe	67
IT-Sicherheit + DV-Technik+ Herstelleranfragen	51
Betriebliche/Behördliche DSB	34
Versorgungsunternehmen	32
Vereine und Verbände	32
Versicherungen	27
Datenschutz außerhalb DE/EU	23
Rundfunk, Fernsehen, Presse	18
Forschung , Statistik	14
Steuerwesen	10
Ausländerrecht	10
Sonstige Themen < 10 (z. B. Religionen und Glaubensgemeinschaften, Landwirtschaft und Forsten, Geodaten)	68
Gesamtsumme dokumentierter Eingaben und Beratungen	**2.189**
davon Summe der dokumentierten Eingaben	2.001
davon Summe der dokumentierten Beratungen	188
davon Eingaben und Beratungen Videobeobachtung betreffend	260
Summe telefonischer Eingaben und Beratungen	**5.808**
Gesamtsumme Eingaben und Beratungen	**7.997**

1.4.2
Sanktionen

Im Berichtsjahr wurden 16 Bußgeldverfahren abgeschlossen. Damit konnte leider wiederum nur ein Teil der Rückstände, die schon im letzten Jahr durch die Belastungen im Rahmen der Umsetzungsarbeiten zur EU-Datenschutzreform entstanden, abschließend bearbeitet werden. In diesem Jahr habe ich erstmals von der Möglichkeit einer Verwarnung gemäß § 56 OWiG Gebrauch gemacht. Dies betraf insbesondere Fälle, in denen der jeweilige Verstoß gegen das BDSG weniger schwerwiegend war und bei denen darüber hinaus eine lange Bearbeitungszeit berücksichtigt wurde.

Den abgeschlossenen Verfahren lagen in sieben Fällen Verstöße gegen Pflichten der verantwortlichen Stellen gegenüber Betroffenen bzw. der Aufsichtsbehörde oder Verstöße gegen Meldeverpflichtungen zugrunde (Tatbestände des § 43 Abs. 1 BDSG). Die übrigen zehn Verfahren bezogen sich auf Vorfälle wegen unzulässiger Datenverarbeitung (Tatbestände des § 43 Abs. 2 BDSG). Elf Verfahren wurden mit einem Bußgeldbescheid oder einer Verwarnung beendet. Insgesamt habe ich Bußgelder bzw. Verwarnungen in Höhe von 16.000 EUR verhängt.

1.4.3
Informationspflicht nach § 42a BDSG

Im Berichtsjahr gingen bei mir insgesamt 85 Mitteilungen nichtöffentlicher Stellen über Vorfälle unrechtmäßiger Kenntniserlangung von Daten durch Dritte nach § 42a BDSG ein. Da die Meldungen zunächst auf einer Selbsteinschätzung der jeweiligen Stellen beruhen, ob eine schwerwiegende Beeinträchtigung von Rechten oder schutzwürdigen Interessen Betroffener droht, stellte sich in 28 Fällen (Verdachtsfälle) nach meiner Prüfung heraus, dass eine solche Gefahr tatsächlich nicht bestand. In 57 Fällen drohte dagegen eine schwerwiegende Beeinträchtigung von Rechten oder schutzwürdigen Interessen Betroffener bzw. war sogar eingetreten. Die jeweiligen Sachverhalte sind nachstehender Tabelle zu entnehmen. In all diesen Fällen haben die verantwortlichen Stellen entsprechend ihrer gesetzlichen Verpflichtung nach § 42a BDSG angemessene Maßnahmen ergriffen, die Daten zu sichern, Betroffene zu informieren, etwaige nachteilige Folgen zu verhindern bzw. zu mindern und eine umfängliche Aufklärung des Vorfalles zu ermöglichen.

Sachverhalt unrechtmäßiger Kenntniserlangung	**Anzahl 2017**
Diebstahl von Kontounterlagen/ Kundenunterlagen	1
Fehlerhafte Übermittlung von Kontodaten an Dritte	2
Fehlversand von Post mit Kontodaten	6
Fehlversand einer E-Mail mit personenbezogenen Daten diverser Kunden	2
Einsichtnahme auf Kontodaten eines Dritten beim Online-Banking	1
Hackerangriff	7
Diebstahl von Laptops mit Kundendaten	1
Diebstahl Electronic-Cash Terminal	25
Fehlversand von Post mit personenbezogenen Daten gemäß § 3 Abs. 9 BDSG	3
Übermittlung personenbezogener Daten an unberechtigte Dritte	3
Zugriff auf Mitarbeiterdaten für die Belegschaft möglich	1
Kundenunterlagen in Müllcontainern gefunden	1
Fehlversand von Schreiben mit Gesundheitsdaten	1
Verlust eines Datenträgers mit personenbezogenen Daten	1
Fehlversand von Schreiben mit Gewerkschaftsdaten	2
Gesamtzahl der begründeten Meldungen	**57**

2. Spezifische Auswirkungen der DS-GVO

2.1
Einschränkung der Prüfbefugnis des HDSB im Bereich der Berufsgeheimnisträger

Ab dem 25.05.2018 gilt die Europäische Datenschutz-Grundverordnung. Dies macht eine Anpassung des nationalen Rechts erforderlich. Davon betroffen ist auch meine Prüfbefugnis.

Die neue Gesetzeslage und die Auswirkungen auf die Prüfbefugnis des HDSB

Die Prüfbefugnis gegenüber Berufsgeheimnisträgern wurde beschränkt. So heißt es in § 29 Abs. 3 BDSG-neu:

> Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuches genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchtstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

Künftige Prüfungen werden dadurch erheblich erschwert. Gerade im Gesundheitsbereich ist es oftmals wichtig, einrichtungsübergreifende Zusammenhänge zu verstehen und dabei auch mittels Einblicke in sensible Daten betroffener Patienten (z. B. Patientenakten) eine Vorstellung von der täglichen Tätigkeit zu bekommen. Mit den bisherigen Aufsichtsbefugnissen, die erforderliche Einsichtnahme zulassen, konnte eine Sachverhaltsaufklärung umfassender und genauer erfolgen. Zum Beispiel konnte ich mir im Kontext der Prüfung einer externen Abrechnungsstelle auch Patientenakten vorlegen lassen, die regelmäßig von entsprechenden Krankenhäusern an die externe Abrechnungsstelle zur Abrechnung übersandt wurden. Ich konnte dadurch feststellen, dass der Umfang gerade bei ambulanten Behandlungsfällen vielfach zu groß und eine Einschränkung angezeigt war. Dementsprechend konnte auch die Beratung der verantwortlichen Stellen gezielter und auch umfangreicher erfolgen.

Entsprechende Probleme dürften sich durch die Einschränkung der Untersuchungsbefugnisse auch bei der Prüfung eines Praxisinformationssystems ergeben, da nunmehr künftig nur

noch mittels Musterfällen Einsicht genommen werden kann und nicht mehr in die aktuelle Fassung des täglichen Arbeitsbetriebes. Auch in den Fällen, in denen z. B. Patientenakten einer Arztpraxis im öffentlichen Raum aufgefunden werden, bleibt es fraglich, inwiefern sich der Hessische Datenschutzbeauftragte noch dieser Problematik annehmen kann, ohne im Sinne der Neuregelung unbefugt Einsicht zu nehmen.

Die neue Regelung ändert allerdings nichts daran, dass ich im privaten Bereich einzelfallbezogen Einsicht in die Akten eines Berufsgeheimnisträgers erhalten kann, wenn die betroffene Person mir eine entsprechende Einwilligung hierzu erteilt. Gleichermaßen werde ich künftig auch den Datenschutzbeauftragten des jeweiligen Berufsgeheimnisträgers verstärkt in meine Prüfungen einbeziehen und ihn um entsprechende Auswertungen ohne Personenbezug bitten, sofern ich beispielsweise einen Überblick über die gängige Praxis im Umgang mit den dort geführten Akten benötige.

Bei der Neugestaltung des Hessischen Datenschutzgesetzes habe ich ausdrücklich auf eine abweichende Regelung hingewirkt. Entsprechend wurde im Entwurf eine Regelung, wie sie das BDSG vorsieht, nicht übernommen. Sofern öffentliche Stellen betroffen sind, kann ich nach wie vor Akteneinsicht in die dort vorhandenen Vorgänge nehmen und meine Prüfungen umfassend durchführen.

2.2
Bußgelder nach DS-GVO und BDSG-neu

Die Schaffung der teilweise noch offenen Rahmenbedingungen für die Festsetzung der neuen Bußgelder nach der DS-GVO ging im Berichtsjahr voran. Auf der EU-Ebene lag der Fokus auf der Planung zur Erarbeitung von Leitlinien zur Bußgeldfestsetzung i. S. v. Art. 70 lit. k) DS-GVO.

2.2.1
National

Deutschland hat auf Bundesebene eine erste Anpassungsphase durchlaufen. Das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU) vom 30.06.2017 (BGBl. I S. 2097) wird am 25.05.2018 in Kraft treten und mit ihm das BDSG-neu.

Mit diesem Gesetz hat der deutsche Gesetzgeber im BDSG-neu von den Öffnungsklauseln in Art. 83 Abs. 7, 8 und nach Art. 84 DS-GVO Gebrauch gemacht.

a) Geldbußen gegen öffentliche Stellen

Nach Art. 83 Abs. 7 DS-GVO kann der nationale Gesetzgeber darüber entscheiden, ob und in welchem Umfang Bußgelder gegen Behörden verhängt werden können. Der Bundesgesetzgeber hat sich bereits gegen das „Ob“ entschieden. Nach § 43 Abs. 3 BDSG-neu können gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Abs. 1 BDSG-neu keine Geldbußen verhängt werden.

Davon zu unterscheiden sind die öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen. Diese fallen nicht unter die öffentlich-rechtlichen Stellen, sondern unter die nichtöffentlichen Stellen im Sinne des BDSG-neu. In Hessen hat der Landesgesetzgeber im Rahmen der Reform des Hessischen Datenschutzgesetzes noch zu entscheiden, ob es Bußgeldverfahren gegen Behörden geben soll. In dem im Dezember 2017 vorgelegten Entwurf ist keine Regelung enthalten.

b) Weitere Bußgeldvorschriften (§ 43 BDSG-neu)

Der nationale Gesetzgeber hat in § 43 BDSG-neu weitere Bußgeldtatbestände aufgenommen. § 43 Abs. 1 BDSG-neu gibt die Bußgeldtatbestände des § 43 Abs. 1 Nr. 7a und b BDSG a. F. wieder. Diese Tatbestände setzen Art. 9 der Verbraucherkreditrichtlinie 2008/48/EG um. Für diese Verstöße wird der bisherige Bußgeldrahmen aus § 43 Abs. 3 S. 1 BDSG a. F. von bis zu 50.000 EUR beibehalten.

c) Angemessene Verfahrensgarantien (§ 41 BDSG-neu)

Nach Art. 83 Abs. 8 DS-GVO muss die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß Art. 83 DS-GVO angemessenen Verfahrensgarantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren unterliegen. Die bestehenden Vorschriften über das Bußgeld- und Strafverfahren sind mit Einschränkungen in § 41 BDSG-neu für anwendbar erklärt worden.

Abweichend von § 2 Abs. 2 des Gesetzes über Ordnungswidrigkeiten (OWiG) erstreckt sich nun das OWiG nach § 41 Abs. 1 BDSG-neu auch auf Verstöße nach Art. 83 Abs. 4 bis 6 der DS-GVO. Allerdings werden Vorschriften aus dem OWiG von der Anwendung ausgenommen. Das sind nach § 41 Abs. 1 BDSG-neu:

– § 17 OWiG (Höhe der Geldbuße),
– § 35 OWiG (Verfolgung und Ahndung durch die Verwaltungsbehörde) und
– § 36 OWiG (Örtliche Zuständigkeit der Verwaltungsbehörde).

Außerdem sind gemäß § 41 Abs. 2 BDGS-neu ausgeschlossen:
– § 56 OWiG (Verwarnung durch die Verwaltungsbehörde),
– § 57 OWiG (Verwarnung durch Beamte des Außen- und Polizeidienstes),
– § 58 OWiG (Ermächtigung zur Erteilung der Verwarnung),
– § 87 OWiG (Anordnung von Einziehung und Verfall),
– § 88 OWiG (Festsetzung der Geldbuße gegen juristische Personen und Personenvereinigungen),
– § 99 OWiG (Vollstreckung von Nebenfolgen, die zu einer Geldzahlung verpflichten) und
– § 100 OWiG (Nachträgliche Entscheidungen über die Einziehung).

Nach § 41 Abs. 2 S. 3 BDSG-neu findet § 69 Abs. 4 S. 2 OWiG mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann. Damit wird der Unabhängigkeit der Aufsichtsbehörde Rechnung getragen und auch der bisher unbefriedigenden Situation, dass aus Sicht der Aufsichtsbehörde berechtigte Ordnungswidrigkeitenverfahren ohne Beteiligung der Aufsicht und ggf. ohne Mitteilung an die Aufsicht eingestellt wurden.

Die Einschränkungen in der Anwendbarkeit des Gesetzes über die Ordnungswidrigkeiten waren erforderlich, da es sonst zu Kollisionen mit den Regelungen der DS-GVO gekommen wäre. Offen und umstritten ist nach wie vor die Frage, ob die §§ 9, 30 und 130 OWiG hätten ausgeschlossen werden müssen. Im Entwurf zum Stand: Beteiligung Länder/Verbände (23.11.2016 09:18) waren die Normen jedenfalls noch ausgeschlossen. Begründet wurde dies damit, dass die DS-GVO hinsichtlich der Frage der Zurechnung von Handlungen abschließend sei. Im Laufe des Gesetzgebungsverfahrens in 2017 ist dieser Passus gestrichen worden. Das verabschiedete BDSG-neu erklärt §§ 9, 30 und 130 OWiG für anwendbar. Damit wird voraussichtlich die Zurechenbarkeit von Ordnungswidrigkeiten erschwert. Inwieweit diese Entscheidung des Gesetzgebers europarechtskonform ist, wird die Praxis zeigen müssen.

Im Kontext mit den angemessenen Verfahrensgarantien ist auch § 43 Abs. 4 BDSG-neu zu nennen. Absatz 4 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung und ist dem § 42a BDSG a. F. entlehnt.

d) Strafvorschriften

Der nationale Gesetzgeber hat von der Öffnungsklausel aus Art. 84 Abs. 1 DS-GVO in § 42 BDSG-neu Strafvorschriften aufgenommen. Für die dort aufgeführten Tatbestände sind Freiheitsstrafen von bis zu zwei bzw. drei Jahren vorgesehen.

e) Kurzpapiere der DSK

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat zur ersten Orientierung eine Reihe von Kurzpapiere zur DS-GVO herausgegeben. Kurzpapier Nr. 2 (s. a. Ziff. 19.2) beschäftigt sich mit den Aufsichtsbefugnissen und Sanktionen.

2.2.2
EU-Ebene

Die Artikel 29-Gruppe hat in ihrer 112. Plenarsitzung im Dezember 2017 die Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 (wp253; http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083) angenommen.

Das Dokument wp253 ist für die Verwendung durch die Aufsichtsbehörden vorgesehen. Es dient der besseren Anwendung und Durchsetzung der DS-GVO und drückt das gemeinsame Verständnis der Bestimmungen von Art. 83 Abs. 2 der Verordnung sowie seine Wechselwirkung mit den Art. 58 und 70 und den entsprechenden Erwägungsgründen aus. Die Leitlinien in wp253 sind nicht erschöpfend. Sie befassen sich mit der Frage der Entscheidung der Aufsichtsbehörde, ob ein Bußgeld verhängt werden soll. Für die Entscheidung über die Höhe des Bußgelds sollen nun in einer Phase 2 ebenfalls Leitlinien erarbeitet werden.

Daher wurde die Enforcement Subgroup von der Artikel 29-Gruppe damit beauftragt, eine Task-Force einzurichten, deren Arbeit auf die Harmonisierung der Berechnung von Bußgel-

dern gerichtet ist (Task-Force Fining Guidelines). Die deutschen Bundesländer sind durch Berlin und stellvertretend durch Niedersachsen sowie meine Behörde in der Task-Force Fining Guidelines vertreten. Die Kick-off-Sitzung der Task Force Fining Guidelines wurde Mitte Dezember in Brüssel durchgeführt.

Im Übrigen verweise ich auf meine Ausführungen im 45. TB auf S. 32 ff.

2.3
Behördliche und betriebliche Datenschutzbeauftragte im Kontext der DS-GVO

Obwohl die in den Art. 37 bis 39 DS-GVO enthaltenen Regelungen sowie die ergänzenden Regelungen des BDSG-neu die Rechtsfigur der oder des Datenschutzbeauftragten nicht neu kreieren, sondern an bereits bekannte und bewährte Regelungen anknüpfen, erhielt ich im Berichtszeitraum vielfältige Anfragen hierzu. Ich habe daher eine Handreichung erarbeitet, die die Voraussetzungen der Benennung, die persönlichen Anforderungen an Datenschutzbeauftragte, ihre Aufgaben, Pflichten und Stellung vor dem Hintergrund der zukünftigen Regelungen beleuchtet.

Die DS-GVO löst ab dem 25.05.2018 die derzeit noch geltenden Regelungen in §§ 4f und 4g BDSG ab. Zukünftig sind die zentralen Regelungen zur Benennung, Stellung und zu den Aufgaben der Datenschutzbeauftragten in den Art. 37 bis 39 DS-GVO enthalten. Zudem sind für betriebliche und behördliche Datenschutzbeauftragte die Vorschriften des BDSG-neu (§§ 5 bis 7 und 38 BDSG-neu) und für behördliche weiter die jeweiligen – sich derzeit in Überarbeitung befindlichen – Landesdatenschutzgesetze zu berücksichtigen.

Im Folgenden möchte ich die 12 Kernpunkte des Papiers, das unter https://www.datenschutz.hessen.de/download.php?download_ID=373&download_now=1 abgerufen werden kann, kurz zusammenfassen.

2.3.1
Keine erleichterte Abberufung oder Kündigung bereits bestellter Datenschutzbeauftragter durch die Neu-Regelung

Grundsätzlich können bereits vor Inkrafttreten der DS-GVO bestellte Datenschutzbeauftragte nicht mit Verweis auf die neuen gesetzlichen Bestimmungen abberufen oder gekündigt werden. Um die Datenschutzbeauftragten mit der zukünftigen Rechtslage vertraut zu machen, müssen Arbeitgeber bzw. Dienstherren bereits bestellte Datenschutzbeauftragte ausreichend Ressourcen (d h. Fortbildungsmaßnahmen, Lehrmaterial, Zeitschriften etc.) zur Verfügung stellen.

2.3.2
Benennungspflicht

Gemäß Art. 37 Abs. 1 lit. a DS-GVO und § 5 Abs. 1 BDSG-neu müssen öffentliche Stellen grundsätzlich eine Datenschutzbeauftragte bzw. einen Datenschutzbeauftragten benennen. Neben den Tatbestandsvoraussetzungen der Benennung nach Art. 37 Abs. 1 lit. b und c DS-GVO für betriebliche Datenschutzbeauftragte gilt aufgrund der Öffnungsklausel des Art. 37 Abs. 4 Satz 1 DS-GVO auch weiterhin die quantitative Benennungspflicht bei mehr als zehn beschäftigten Personen, die ständig mit automatisierter Verarbeitung personenbezogener Daten befasst sind. Von der Möglichkeit der Öffnungsklausel des Art. 37 Abs. 4 Satz 1 DS-GVO hat der deutsche Gesetzgeber zudem für Stellen, die einer Datenschutz-Folgenabschätzung unterliegen oder die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- und Meinungsforschung nutzen, Gebrauch gemacht und in § 38 Abs. 1 BDSG-neu in Ergänzung zu Art. 37 Abs. 1 DS-GVO die Pflicht zur Benennung einer oder eines Datenschutzbeauftragten näher normiert.

2.3.3
Benennungspflicht für Verantwortliche und Auftragsverarbeiter

Sowohl Verantwortliche als auch Auftragsverarbeiter müssen nach Art. 37 Abs. 1 DS-GVO und § 38 Abs. 1 BDSG-neu eine oder einen Datenschutzbeauftragten benennen. Aus deutscher Sicht handelt es sich mithin um eine Erweiterung der bisher bestehenden Bestellpflicht, da bisheriger Normadressat des BDSG nur die verantwortliche Stelle ist.

2.3.4
Veröffentlichungs- und Mitteilungspflicht

Nach Art. 37 Abs. 7 DS-GVO sind die Kontaktdaten der bzw. des Datenschutzbeauftragten durch die Verantwortlichen und die Auftragsverarbeiter zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Zur erforderlichen Meldung beachten Sie bitte meinen Beitrag in diesem Tätigkeitsbericht unter Ziff. 2.4.

2.3.5
„Konzernprivileg“ für Benennung

Die DS-GVO schafft in Art. 37 Abs. 2, Abs. 3 DS-GVO und § 5 Abs. 2 BDSG-neu für Verantwortliche und Auftragsverarbeiter die Möglichkeit der Benennung einer oder eines Datenschutzbeauftragten für eine Unternehmensgruppe, vorausgesetzt diese bzw. dieser kann von jeder Niederlassung leicht erreicht werden. Zukünftig ist daher eine separate Benennung für jedes einzelne Konzernunternehmen nicht mehr zwingend erforderlich. Im Verhältnis zur bisherigen Regelung des BDSG handelt es sich somit um eine Erleichterung der formalen Anforderungen. Unter dem Begriff der leichten Erreichbarkeit ist zum einen die Sicherstellung der persönlichen Kommunikation durch ausreichend verfügbare Kontaktmöglichkeiten, z. B. die Einrichtung eines Kontaktformulars auf der Webseite, Bereitstellung einer Telefonnummer und/oder E-Mail-Adresse, regelmäßige Sprechstunden für Beschäftigte zu verstehen, zum anderen müssen Datenschutzbeauftragte in der Lage sein, mit Aufsichtsbehörden und Betroffenen sprachlich zu kommunizieren.

2.3.6
Interne oder externe Benennung möglich

Datenschutzbeauftragte können sowohl Beschäftigte benennpflichtiger Unternehmen sein als auch auf der Grundlage von Dienstleistungsverträgen tätig werden. Diese Wahlfreiheit wird für öffentliche Stellen durch die Vorschriften Art. 37 Abs. 6 DSG-VO und § 5 Abs. 4 BDSG-neu neu eingeführt, für Unternehmen ist dies aktuell bereits gegeben (vergleiche § 4f Abs. 2 Satz 3 und 4 BDSG).

2.3.7
Datenschutzteam und Benennung juristischer Personen

Neben der Benennung einer einzelnen Person als Datenschutzbeauftragte bzw. Datenschutzbeauftragter ist es auch möglich, dass mehrere Personen gemeinsam die Aufgaben der bzw. des Datenschutzbeauftragten wahrnehmen. Auch die Benennung einer juristischen Person zum Datenschutzbeauftragten ist nach Ansicht der WP 29 zulässig. Diese hat hierzu im Dezember 2016 das Working Paper 243 „Guidelines on Data Protection Officers (‘DPOs’)“ veröffentlicht. Aktuell vertreten die deutschen Aufsichtsbehörden hierzu noch unterschiedliche Auffassungen. Aus meiner Sicht ist eine solche Gestaltung der Position der bzw. des Datenschutzbeauftragten denkbar. Wie sichergestellt werden kann, dass eine solche Konstruktion allen Anforderungen genügt, ist im Einzelfall zu klären.

2.3.8
Freiwillige Benennung

Im Falle der freiwilligen Benennung betrieblicher Datenschutzbeauftragter gelten sämtliche Vorschriften des vierten Abschnitts der DS-GVO. Zu beachten ist aber, dass der zur DS-GVO hinzutretende Abberufungs- und Kündigungsschutz nach dem Wortlaut des § 38 Abs. 2 BDSG-neu nur bei der verpflichtenden Benennung zur Anwendung gelangt. Sofern der Abberufungs- und Kündigungsschutz dennoch zur Anwendung gelangen sollen, bedarf es einer entsprechenden Regelung zwischen den Parteien.

2.3.9
Persönliche Anforderungen an den Datenschutzbeauftragten

Sowohl die DS-GVO als auch das BDSG-neu verlangen, dass die Auswahl und Benennung von Datenschutzbeauftragten auf der Grundlage folgender drei Voraussetzungen erfolgt:

1. berufliche Qualifikation,
2. Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis,
3. Fähigkeit zur Erfüllung der in der DS-GVO bzw. BDSG-neu genannten Aufgaben.

Zu fordern sind hiernach jedenfalls Kenntnisse des nationalen und europäischen Datenschutzrechts und ein vertieftes Verständnis der DS-GVO, wobei sich das konkret zu fordernde Fach-

wissen an der Sensitivität, Komplexität und dem Umfang der Verarbeitungsvorgänge orientieren sollte. Auch das Betätigungsfeld verantwortlicher Stellen oder Auftragsverarbeitern und die hiermit verbundenen Datenverarbeitungsvorgänge (z. B. Gesundheitsdatenschutz, Beschäftigtendatenschutz oder Kundendatenschutz) können bei der Frage des erforderlichen Fachwissens der Datenschutzbeauftragten eine besondere Rolle spielen.

Über die berufliche und fachliche Qualifikation hinaus verlangt die WP 29 im Zusammenhang mit der Fähigkeit zur Erfüllung der in der DS-GVO genannten Aufgaben, dass Datenschutzbeauftragte ein hohes Maß an persönlicher Integrität und Berufsethik aufweisen (siehe hierzu Working Paper 243, Seite 12).

2.3.10
Aufgaben und Pflichten

Bei einer Gesamtschau der Regelungen der DS-GVO sowie des BDSG-neu lassen sich die folgenden Kernaufgaben für Datenschutzbeauftragte zusammenfassen:

1. Unterrichtung und Beratung,
2. Überwachung der Einhaltung der DS-GVO und anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten (oder des BDSG-neu und sonstiger Vorschriften über den Datenschutz)/Zuweisung von Zuständigkeiten,
3. Sensibilisierung und Schulung,
4. Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
5. Zusammenarbeit mit der Aufsichtsbehörde,
6. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

Die DS-GVO bzw. das BDSG-neu sind nicht nur beschreibender Aufgabenkatalog, sondern geben Datenschutzbeauftragten auch gleich eine Maxime zur Aufgabenerfüllung mit auf den Weg: Datenschutzbeauftragte tragen bei der Erfüllung ihrer Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie dabei die Art und den Umfang, die Umstände und Zwecke der Verarbeitung berücksichtigen.

Überdies steht es Behörden und Unternehmen frei, die Rolle der Datenschutzbeauftragten strategischer und proaktiver auszugestalten, als dies in der DS-GVO und dem BDSG-neu vorgesehen ist, da die Vorschriften keine abschließende Aufgabenzuweisung enthalten.

2.3.11
Stellung des Datenschutzbeauftragten

Von ausschlaggebender Bedeutung für eine wirkungsvolle Tätigkeit ist die unabhängige und organisatorisch herausgehobene Stellung der Datenschutzbeauftragten, da sie andernfalls den zuvor beschriebenen Aufgaben und Pflichten nur schwerlich gerecht werden können.
Folgende Themenkreise zur Stellung der Datenschutzbeauftragten in Behörden und Unternehmen können zusammengefasst werden:

1. ordnungsgemäße und frühzeitige Einbindung der Datenschutzbeauftragten,
2. Bereitstellung erforderlicher Ressourcen,
3. Weisungsfreiheit und Unabhängigkeit,
4. keine Benachteiligung: Abberufungs- und Kündigungsschutz,
5. unmittelbarer Berichtsweg zur höchsten Führungsebene,
6. Anrufungsrecht der Betroffenen,
7. kein Interessenkonflikt,
8. Zusammenarbeit mit der Aufsichtsbehörde.

Kernstück der Unabhängigkeit der Datenschutzbeauftragten ist die Weisungsfreiheit. Sie ist nach der DS-GVO und dem BDSG-neu auf solche Handlungen beschränkt, die sich auf die Ausübung der Aufgaben der Datenschutzbeauftragten beziehen.

Unternehmen und Behörden dürfen Datenschutzbeauftragten gegenüber somit keine Weisungen in ihrer Funktion als Datenschutzbeauftragte erteilen. Aus diesem Grund sind z. B. Vorgaben zur Erreichung eines bestimmten Ziels, zur Art und Weise der Bearbeitung von Beschwerden oder zum Austausch mit Aufsichtsbehörden unzulässig.

Der deutsche Gesetzgeber hat sich für eine Stärkung der Unabhängigkeit der Datenschutzbeauftragten entschieden. Das BDSG-neu enthält daher die Regelung, dass eine Abberufung nur in entsprechender Anwendung des § 626 BGB möglich und Kündigungen nur aus wichtigem Grund zulässig sind. Darüber hinaus ist nach dem BDSG-neu eine Kündigung des Arbeitsverhältnisses nach dem Ende der Tätigkeit als Datenschutzbeauftragte oder als Datenschutzbeauftragter innerhalb eines Jahres nach der Abberufung unzulässig, es sei denn, die kündigende Stelle ist zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt.

Die bereits aus dem aktuellen BDSG bekannten Privilegierungen bleiben somit bestehen.

2.3.12
Sanktionen und Haftung

Verstöße gegen die gesetzlichen Regelungen zu Datenschutzbeauftragten können zukünftig mit Geldbußen von bis zu 10.000.000 EUR oder im Falle eines Unternehmens bis zu 2% seines gesamten, weltweit erzielten Jahresumsatzes geahndet werden, je nachdem, welcher Betrag höher ist. Verglichen mit den aktuell anzuwendenden Bußgeldtatbeständen des BDSG zeigt sich, dass sich mit der Neuregelung des Art. 83 DS-GVO eine erhebliche Sanktionsverschärfung für Verantwortliche und Auftragsverarbeiter ergibt.

Aufgrund des zukünftigen Aufgabenkatalogs, der deutlich erweiterten Kontroll-, Hinweis- und Beratungspflichten der Datenschutzbeauftragten, wurde in den vergangenen Monaten vermehrt diskutiert, ob hiermit auch eine weitergehende Haftung und Verantwortlichkeit der Datenschutzbeauftragen einhergeht. Die WP 29 hat sich hierzu bereits im Working Paper 243 positioniert und führt aus, dass Überwachung der Einhaltung der gesetzlichen Bestimmungen nicht bedeute, dass Datenschutzbeauftragte automatisch auch persönlich verantwortlich seien, wenn ein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt werde. Die Einhaltung des Datenschutzes sei vielmehr die unternehmerische Pflicht der Verantwortlichen/Auftragsverarbeiter und nicht der Datenschutzbeauftragten. Verantwortlich bleiben daher in erster Linie die Verantwortlichen oder Auftragsverarbeiter.

Soweit Datenschutzbeauftragte jedoch die ihnen von der DS-GVO und dem BDSG-neu unmittelbar übertragenen Aufgaben nicht erfüllen, kann, ganz unabhängig von der Umsetzungsverantwortung, unter Umständen auch eine persönliche Haftung der Datenschutzbeauftragten in Betracht kommen. Es wird daher den Datenschutzbeauftragten dringend empfohlen, eigenständig die Beratungs- und Überwachungsmaßnahmen zu dokumentieren, um nachweisen zu können, dass sie die ihnen obliegenden Aufgaben ordnungsgemäß erfüllen.

2.4
Meldung von Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO

Aufgrund der Europäischen Datenschutzreform sind hessische Verantwortliche und Auftragsverarbeiter ab dem 25.05.2018 gem. Art. 37 Abs. 7 DS-GVO verpflichtet, die Kontaktdaten der oder des Datenschutzbeauftragten zu veröffentlichen und diese dem Hessischen Datenschutzbeauftragten mitzuteilen. Verstöße gegen die Veröffentlichungs- und Mitteilungspflicht können mit einem Bußgeld geahndet werden.

Adressat dieser Regelung sind Verantwortliche und Auftragsverarbeiter und nicht die bzw. der benannte Datenschutzbeauftragte. Unterbleibt die Meldung oder ist sie fehlerhaft, erfüllt dies den Bußgeldtatbestand des Art. 83 Abs. 4 lit. a DS-GVO.

Um einen reibungslosen Ablauf für die Vielzahl der erwarteten Meldungen zu gewährleisten, strebe ich die Implementierung eines automatisierten Meldeverfahrens auf meiner Internetseite an. Zur Mitteilung der Kontaktdaten des Datenschutzbeauftragten werde ich rechtzeitig vor dem 25.05.2018 weitergehende Informationen auf meiner Internetseite veröffentlichen.

2.5
Datenschutz-Grundverordnung und aktuelle Entwicklungen in der Versicherungswirtschaft

Die Datenschutz-Grundverordnung zwingt die Versicherungsbranche, ihre Geschäftstätigkeiten datenschutzrechtlich zu überarbeiten. Dies gilt insbesondere auch mit Blick auf die Arbeit von Auskunfteien in der Versicherungswirtschaft.

Aktuelle Situation

Die Versicherungsbranche ist dabei, ihre Geschäftstätigkeiten der DS-GVO anzupassen. Hauptansprechpartner der Datenschutzaufsichtsbehörden ist der Gesamtverband der Deutschen Versicherungswirtschaft mit Sitz in Berlin (GDV e. V.), aber zurzeit auch der Verband der Privaten Krankenversicherung in Köln (PKV e. V.).

Dieser Verband plant, wie es schon in den übrigen Versicherungssparten seit langem der Fall ist, ebenfalls ein Hinweis- und Informationssystem (HIS) in Form einer Auskunftei zu errichten, um insbesondere der missbräuchlichen Inanspruchnahme von Privaten Krankenversicherungen entgegenzuwirken.

Es geht also darum, wie in den anderen Versicherungsbereichen, eine Auskunftei zu errichten, die unter Beachtung des Rechts auf informationelle Selbstbestimmung der Betroffenen die schützenswerten Interessen der Versicherer (und der Versichertengemeinschaft) angemessen berücksichtigt.

Wirtschaftliche Handlungsfreiheit der Versicherungsunternehmen und Datenschutz

Datenschutzrecht ist in erster Linie Abwägungsrecht. Das Recht auf informationelle Selbstbestimmung muss im Wege eines angemessenen Ausgleichs mit anderen ebenfalls schützenswerten Interessen ausbalanciert werden.

Die mitunter in der öffentlichen Debatte geäußerte Ansicht, bloße Geschäfts- und Gewinninteressen der Privatwirtschaft dürften den Datenschutz nicht kommerzialisieren, vernachlässigt die verfassungsrechtliche Ausgangslage. Denn das Grundgesetz schützt auch Privatunternehmen mit Blick auf ihre wirtschaftliche Betätigung, neben dem Datenschutz der Betroffenen. Deren „Interesse an informationeller Selbstbestimmung steht das gleichfalls erhebliche Offenbarungsinteresse des Versicherers gegenüber, das in der Vertragsfreiheit wurzelt und damit ebenfalls grundrechtlichen Schutz durch Art. 12 GG genießt...“, heißt es in einem jüngeren Urteil des Bundesgerichtshofs unter Verweis auf die Rechtsprechung des Bundesverfassungsgerichts (Urt. v. 13.07.2016 – IV ZR 292/14 = r+s 2016, 475 Nr. 31).

Dementsprechend ist neben der datenschutzrechtlichen Vereinheitlichung im Europäischen Binnenmarkt ein angemessener Ausgleich zwischen Datenschutz einerseits und Privatautonomie der Unternehmen andererseits das zentrale Anliegen der Datenschutz-Grundverordnung. Im Übrigen ist es gerade auch ein Ausdruck informationeller Selbstbestimmung, wenn die Betroffenen dieses Recht ihrerseits auch kommerziell nutzen, etwa um Vergünstigungen für eine risikoarme Fahrweise (pay as you drive) oder für einen gesundheitsorientierten Lebensstil (Gesundheits-Apps) versicherungsvertraglich zu erreichen. Entscheidend ist hier die seriöse Information der Betroffenen, also Transparenz, sowie Freiwilligkeit als eine Essentiale der Selbstbestimmung.

Die Datenschutz-Grundverordnung orientiert sich im Wesentlichen an dem bisherigen deutschen Datenschutzrecht, was den Anpassungsbedarf etwa der Verhaltensregeln (Art. 40 DS-GVO) der Versicherungswirtschaft insofern erleichtert, als ja nicht mit den Grundprinzipien des bisherigen Datenschutzrechts gebrochen wird. In Zukunft wird es sogar gewisse Erleichterungen geben, weil etwa der Grundsatz der Direkterhebung, nämlich das Gebot, die Daten beim Betroffenen zu erheben, in der DS-GVO nicht übernommen worden ist und die Einwilligung des Betroffenen nicht mehr prinzipiell in Schriftform vorliegen muss.

Insgesamt kann man jedenfalls davon ausgehen, dass im Mai 2018 mit der Datenschutz-Grundverordnung kompatible Verhaltensregeln der deutschen Versicherungswirtschaft vorliegen werden.

2.6
Datenschutz-Folgenabschätzung nach DS-GVO: Was kann durch sie geleistet werden?

Mit der Datenschutz-Folgenabschätzung ist ein Verfahren zu konkretisieren, das von einer Risikobewertung zur Reduktion eines hohen Risikos für Rechte und Freiheiten betroffener Personen führt.

2.6.1
Aktuelle Rahmenbedingungen

Unter der Datenschutz-Folgenabschätzung (DSFA) versteht die Datenschutz-Grundverordnung (DS-GVO) ein Verfahren, mit dem ein hohes Risiko für Rechte und Freiheiten betroffener Personen zu reduzieren ist. Eine DSFA ist durchzuführen, wenn ein Verarbeitungsvorgang neu eingeführt oder geändert wird, insbesondere, wenn neue Technologien eingesetzt werden (Art. 35 Abs. 1 DS-GVO). Dazu sind Art, Umfang, Umstände und Zweck der Verarbeitung zu bewerten, wie auch bei der Verhältnismäßigkeit (Art. 5 DS-GVO), der Rechtmäßigkeit (Art. 6 DS-GVO) und im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) schriftlich niederzulegen.

Verantwortlichen und Auftragsverarbeitern ist jeweils zu empfehlen, die Liste der Verarbeitungsvorgänge gemäß Art. 35 Abs. 4 zu beachten, für die eine DSFA verpflichtend ist. Eine erste solche Liste findet sich in der Stellungnahme, die durch die Artikel 29-Gruppe bereits veröffentlicht ist. Sie ist unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 zu finden. Die Datenschutzaufsichtsbehörden sind europaweit dabei, diese Listen abzustimmen, denn sie sind an den Europäischen Datenschutzausschuss zu melden und können einem Kohärenzverfahren unterliegen.

Als erste bundesweite Auslegungshilfen sind von der Datenschutzkonferenz (DSK) verabschiedete Kurzpapiere heran zu ziehen. Darunter ist auch ein Kurzpapier speziell zum Thema DSFA, das unter Ziff. 19.5 sowie auf meiner Homepage https://www.datenschutz.hessen.de/neuesdatenschutzrecht.htm#entry4971 zu finden ist. Wenn ein Verarbeitungsvorgang voraussichtlich kein hohes Risiko aufweist, ist eine DSFA nicht zwingend erforderlich. In jedem Fall sind die Gründe zu dokumentieren, warum keine DSFA für die betrachteten Verarbeitungsvorgänge vorgenommen wurde.

Zur Klärung und näheren Erläuterung der für eine DSFA bestehenden Anforderungen und zur Bestimmung der Vorgehensweise wurde von der Datenschutzkonferenz (DSK) eine Arbeitsgruppe zur Datenschutz-Folgenabschätzung (DSFA) installiert. Diese Arbeitsgruppe hat neben der Evaluierung und der Etablierung von Verfahren zur DSFA das Ziel, die Vorgehensweise einer datenschutzrechtlichen Bewertung und die Abwägung, was ein hohes Risiko ist, zu bestimmen. An der Arbeitsgruppe der DSK nehmen zwei meiner Mitarbeiterinnen teil.

2.6.2
Ergebnisse zur Durchführung eines Verfahrens

Im Rahmen einer DS-GVO-spezifischen Prüfpraxis sind verschiedene Ansätze möglich. Vor dem technischen Hintergrund, Anforderungen gemäß Art. 35 Abs. 7 zu gewährleisten, sind dies:

– eine systematische Beschreibung der geplanten Verarbeitungsvorgänge,
– die Nennung der Zwecke der Verarbeitung einschließlich der vom Verantwortlichen verfolgten berechtigten Interessen,
– die Bewertung der Notwendigkeit und der Verhältnismäßigkeit und
– Benennung der Maßnahmen, die ergriffen werden, um ein hohes Risiko einzudämmen.

Die Verantwortlichen, die Auftragsverarbeiter und die zuständige Aufsichtsbehörde sehen sich in diesem Zusammenhang mit einer neueren Prüfpraxis konfrontiert. Denn das Verfahren der DSFA ist im Kontext diverser Artikel der DS-GVO zu sehen, die als wesentlichen Kern Anforderungen an eine technische Umsetzung zur datenschutzkonformen Verarbeitung stellen. Dazu gehören insbesondere die Artikel, die sich auf

– das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO),
– Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO),
– die Sicherheit der Verarbeitung (Art. 32 DS-GVO) und
– die Zertifizierung (Art. 42 DS-GVO) beziehen.

Die Reihenfolge, in der diese Artikel aufgezählt sind, deutet ein mögliches Vorgehen aus technischer Perspektive an. Nur aus der zusammenhängenden Betrachtung der genannten Artikel lässt sich eine DSFA durchführen, die insgesamt Abwägungen, Bewertungen und schließlich die Auswahl von zu ergreifenden Maßnahmen zulässt, so dass sich Risiken umfassend reduzieren lassen.

2.6.2.1
Gewährleistungsziele

In der Gesamtheit sind sowohl die bekannten Kontroll- als auch die neueren Gewährleistungsziele zu berücksichtigen.

Gewährleistungsziele gliedern sich in als elementar zu bezeichnende Ziele: Vertrautheit, Verfügbarkeit und Integrität. Die neueren Gewährleistungsziele, die nochmal deutlicher datenschutzrechtliche Fragen ins Zentrum rücken, sind: Transparenz, Nichtverkettbarkeit und Intervenierbarkeit, insbesondere zur Gewährleistung der Rechte betroffener Personen. Die Gewährleistungsziele haben ihre Entsprechungen in verschiedenen bereits genannten Artikeln mit starkem technischem Bezug der DS-GVO, insbesondere Art. 25 und Art. 32. Die Schlüsselbegriffe in diesen Artikeln sind Vertraulichkeit, Verfügbarkeit, Integrität, Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer, so wie eine Zweckbindung.

Das Standard-Datenschutzmodell (SDM) bietet gute Anhaltspunkte. Hierin befinden sich im dazugehörigen Handbuch so genannte generische Maßnahmen, was zu tun ist, um Anforderungen in ein datenschutzrechtliches Konzept zu überführen. Das SDM-Handbuch findet sich z. B. unter https://www.datenschutz.hessen.de/ft015.htm auf meinen Web-Seiten. Ein solches Konzept – wie im SDM – ist grundlegend für die DSFA. Einige Beispiele für generische Maßnahmen zur Reduktion von Risiken bei der Verarbeitung von personenbezogenen Daten sind

– **Verfügbarkeit:** die Umsetzung in ausgewählten, redundant bereitgestellten Systemen oder die Implementierung von Backup-Prozessen;
– **Integrität:** der Einsatz von Authentifikations- und Autorisierungsmechanismen oder auch der Vergleich von Hash-Werten;
– **Vertraulichkeit:** der Einsatz von Verschlüsselungsverfahren, wobei Qualität und Härte der Verfahren zu berücksichtigen sind, wie auch konsequente Umsetzung und Pflege von Berechtigungen durch Rollen und Rechte;
– **Nichtverkettbarkeit:** Trennung der Verfahren, Mandantenfähigkeit von IT-Systemen oder eine Steuerung von Zugriffsmechanismen für spezifizierte Autorisierungen mittels eines Identitätsmanagements;
– **Transparenz mit Perspektive Zweckbindung:** prüffähige Systeme, die z. B. automatisierte Benachrichtigungen generieren oder bei Änderungen von personenbezogenen Daten eine nachvollziehbare, ggf. für die Aktion begrenzte Protokollierung ermöglichen, und

– **Intervenierbarkeit:** ein „Aus-Schalter“ für Teile von Verfahren und ihrer Verarbeitungsvorgänge, ggf. für eine definierte Zeit, wie der Bearbeitungsdauer zur Klärung einer Beschwerde durch eine betroffene Person.

Wie in den Beispielen zu erkennen, werden einige Prozesse und Technologien genannt, die ebenso als technische und organisatorische Maßnahmen zur Unterstützung von Kontrollzielen einsetzbar sind. Alle Kontrollziele sind unter den Gewährleistungszielen zu subsummieren. Der Vorteil der Gewährleistungsziele liegt in ihrer innewohnenden Transzendenz. Verfahren und dazugehörige Verarbeitungsvorgänge werden i. d. R. heute technisch in System-übergreifenden und in Bezug auf die Standorte von Systemen durch Länder- und oftmals Staaten-übergreifende Lösungen ausgeführt. Des Weiteren besteht ein direkter Zusammenhang zu den Art. 13 bis 18 DS-GVO, die Betroffenenrechte implementieren.

2.6.2.2
ISO-Normen aus dem Bereich der IT-Sicherheit

Des Weiteren sind die Aufsichtsbehörden aufgefordert, Verfahren zur Zertifizierung zu fördern (Art. 42 DS-GVO). Im laufenden Anpassungsprozess befinden sich daher auch die ISO-Normen der 2700x-Reihe, die sich auf ein IT-Sicherheitsmanagement-System (ISMS) beziehen. In der Systematik dieser ISO-Normen sind die Konkretisierungen für ein dauerhaft umzusetzendes bzw. zu betreibendes ISMS mit den Bezeichnungen DIN ISO 31000 oder auch DIN ISO 31010 zu nennen. Die technische Norm DIN ISO 31000 beinhaltet ein Risikomanagement (Grundsätze und Management), so dass regelmäßig eine Risikobewertung aus der Sicht der IT-Sicherheit vorgenommen wird. Eine Anleitung bzw. ein Verfahren zur erforderlichen Risikobewertung befindet sich in DIN ISO 31010. In Analogie zu den ISO-Normen und in Teilen datenschutzrechtlichen Anforderungen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die BSI-Standards 200-1 bis 200-3 entwickelt. Diese ersetzen die BSI-Standards 100-1 bis 100-4. Das SDM ist in Bezug auf die Ausrichtung aktuell umzusetzender datenschutzrechtlicher Aspekte in der Technik umfassender als die ISO-Normen aus dem Bereich des ISMS.

2.6.3
Fazit

Ein zentrales Ergebnis eines Workshops der AG Datenschutzfolgenabschätzung im Juni 2017 und in Fortsetzung im September 2017 ist, dass eine adäquate Risikobewertung nur im Zusammenhang mit dem Anwendungskontext möglich ist; d. h. wofür IT-gestützte Prozesse in Bezug auf die Nutzung für Verarbeitungsvorgänge angepasst werden. Eine Anwendungskontext-unabhängige Bewertung eines IT-Produkts wird i. d. R. nicht genügen. Die bisherigen ISO-Normen legen jedoch eine derartige Bewertung nah. Folglich ist festzuhalten: Verantwortliche und Auftragsverarbeiter, die ein ISMS betreiben, sollten das weiterhin tun. Sie sollten aber auch eine datenschutzrechtliche Konkretisierung, z. B. mit Hilfe des SDM, vornehmen.

In der Praxis wird sich erst noch erweisen müssen, inwieweit diese Ansätze tatsächlich ineinandergreifen, um eine datenschutzkonforme Verarbeitung aus technischer Sicht zu gewährleisten. Wesentlich bleibt aber die Beschreibung der Verarbeitungstätigkeiten im Kontext der Anwendung bzw. Sektors, z. B. bei Banken oder im Gesundheitswesen. Diese bereichsbezogene Konkretisierung verschafft Klarheit.

3. Gesetzgebung

3.1
Gesetz zur Förderung des elektronischen Identitätsnachweises

Das Gesetz zur Förderung des elektronischen Identitätsnachweises vom 07.07.2017 ändert das Personalausweis- und Passgesetz sowie das Aufenthaltsgesetz. Erklärtes Ziel der Gesetzesinitiative war die Förderung der Nutzung der eID-Funktion des Personalausweises und des elektronischen Aufenthaltstitels (eAT). Daneben hat der Gesetzgeber dem vermeintlich wachsenden Bedürfnis von Ausweiskopien im privaten und behördlichen Rechtsverkehr Rechnung getragen.

Stärkung der eID-Funktion

Der im Jahr 2010 eingeführte neue Personalausweis und der elektronische Aufenthaltstitel (eAT) besitzen eine Funktion zum elektronischen Identitätsnachweis, die sog. eID-Funktion, die es deutschen Bürgerinnen und Bürgern sowie aufenthaltsberechtigten Ausländern ermöglicht, sich gegenüber Behörden und Unternehmen via Internet auszuweisen. Ich habe darüber ausführlich in meinem 39. Tätigkeitsbericht (Ziff. 3.4) berichtet. In den vergangenen Jahren hat sich gezeigt, dass die praktische Nutzung der eID-Funktion stark hinter den Erwartungen zurückgeblieben ist. Einerseits haben viele Bürger die Funktion bei Ausgabe des Ausweises gleich deaktivieren lassen. Andererseits sahen viele Behörden und Unternehmen in dem Verfahren der Vergabe der Berechtigungszertifikate zum Auslesen der Daten aus den genannten Dokumenten eine zu hohe Hürde, um dieses Identifizierungsverfahren im Rechtsverkehr als attraktiv erscheinen zu lassen.

Um diese Attraktivität zu steigern, hat der Bundesgesetzgeber mit dem o. g. Gesetz die Hürde zur Deaktivierung der eID-Funktion höher gelegt und die Anforderungen an die Vergabe von Berechtigungszertifikaten abgesenkt.

Im Gesetzgebungsverfahren haben die unabhängigen Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung vom 24.01.2017 (s. a. Ziff. 18.1) insbesondere die Pläne hinsichtlich der Vergabe der Berechtigungszertifikate kritisiert:

– „Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass der Diensteanbieter nur die für den jeweili-

gen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

– Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen."

Zwar ist der verabschiedete Gesetzestext datenschutzfreundlicher als der zunächst vorgelegte Gesetzentwurf der Bundesregierung, er setzt aber die o. g. Forderungen der Datenschutzkonferenz (DSK) nur unzureichend um.

§ 21 Abs. 2 PAuswG

Die Berechtigung wird auf Antrag erteilt. Die antragstellende Person muss die Daten nach § 18 Abs. 4 Satz 2 Nummer 1, 2 und 4 angeben. Die Berechtigung ist zu erteilen, wenn

1. der Diensteanbieter seine Identität gegenüber der Vergabestelle für Berechtigungszertifikate nachweist,
2. der Diensteanbieter das dem Antrag zu Grunde liegende Interesse an einer Berechtigung, insbesondere zur geplanten organisationsbezogenen Nutzung darlegt,
3. der Diensteanbieter die Einhaltung des betrieblichen Datenschutzes versichert und
4. der Vergabestelle für Berechtigungszertifikate keine Anhaltspunkte für eine missbräuchliche Verwendung der Daten vorliegen.

Der Diensteanbieter muss daher nicht mehr nachweisen, dass bestimmte zu übermittelnde Daten für den Zweck der Datenverarbeitung auch erforderlich sind. Er muss sogar, anders als nach der alten Rechtslage, den Verwendungszweck überhaupt nicht mehr darlegen. Auch die Nachweispflicht über getroffene Datenschutz- und Datensicherheitsmaßnahmen besteht nur noch eingeschränkt.

Ausweiskopien

Mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises hat der Gesetzgeber auch das Fertigen von Ausweiskopien auf eine neue Rechtsgrundlage gestellt und Paß- und

Personalausweisgesetz geändert. Er hat damit dem wachsenden Bedürfnis von Ausweiskopien im privaten und behördlichen Rechtsverkehr Rechnung getragen.

In den beiden weitgehend gleichlautenden Vorschriften des § 18 Abs. 3 PaßG und § 20 Abs. 2 PAuswG wird nun das Ablichten von Ausweisen beschrieben und im Hinblick auf Zulässigkeiten geregelt.

§ 20 Abs. 2 PAuswG

Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die Daten erhebende oder verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Der Begriff des Ablichtens umfasst die in der Praxis üblicherweise angewandten Techniken zum Herstellen von Kopien, nämlich das Fotografieren, das Scannen und das Fotokopieren eines Personalausweises oder Passes. Das Ergebnis eines solchen Vorganges muss jederzeit als Kopie erkennbar, soweit nicht in schwarz-weiß erstellt, und entsprechend gekennzeichnet sein.

Wenn nicht eine Rechtsvorschrift die Kopie des Ausweises ausdrücklich vorschreibt, ist eine Kopie nur mit Zustimmung des Ausweisinhabers zulässig, die jedoch im Falle einer Verweigerung durchaus negative Konsequenzen für den Ausweisinhaber zur Folge haben kann. Es werden diesbezüglich immer wieder Anfragen an mich gerichtet. Dabei wird häufig argumentiert, dass eine Ausweiskopie für Identifizierungszwecke im beruflichen Bereich erforderlich sei.

Zweifel an einer Identität kann jedoch eine Ausweiskopie nur in dem Maße abhelfen, wie auch der Originalausweis, nämlich durch den unmittelbaren Abgleich des Bildes auf dem Ausweis und dem Ausweisinhaber. Tatsächlich werden Ausweiskopien jedoch im Einverständnis mit dem Ausweisinhaber an Dritte weitergegeben, um dort Identifizierungszwecken zu dienen, ob-

wohl die Kopie dies gar nicht leisten kann. Einen grundsätzlichen Mehrwert bietet eine Ausweiskopie im Vergleich zu gewissenhaft notierten und weitergeleiteten Personaldaten demnach nicht.

Vor dem Hintergrund, dass in Sicherheitsbereichen, die rechtlich normierte Abgleiche von Personalien in Datenbanken erforderlich machen, eine fehlerhafte Erfassung oder Übermittlung weitreichende Folgen haben kann, erscheint hier das einvernehmliche Übermitteln einer Ausweiskopie zum einmaligen Abgleich von Personalien tolerabel. Nach dem erfolgten Abgleich ist diese Kopie dann aber abschließend zu vernichten.

Datenschutzrechtlich problematisch ist, dass in Sicherheitsbereichen eine Verweigerung des Ausweisinhabers zum Fertigen und Weiterleiten einer Ausweiskopie ein Ausschlusskriterium sein kann, und der Ausweisinhaber tatsächlich keinen Entscheidungsspielraum hat, ohne Nachteile in Kauf nehmen zu müssen.

Außerhalb sicherheitsrelevanter Bereiche darf das Fertigen von Ausweiskopien das eigenverantwortliche Notieren von benötigten Personalien weder ersetzen noch ergänzen.

4. Europa und internationaler Datenverkehr

4.1
Internationale Datentransfers – Privacy Shield auf dem Prüfstand

Die Artikel 29-Datenschutzgruppe hat eine Mitarbeiterin des Hessischen Datenschutzbeauftragten als Mitglied einer 8-köpfigen Delegation nominiert, die gemeinsam mit der Europäischen Kommission und dem US-Handelsministerium sowie weiteren US-Behörden die erste Überprüfung des Privacy Shield in Washington D.C. durchgeführt hat.*

In diesem Jahr stand die erste Überprüfung des Privacy Shield an. Diese Überprüfung ist im Regelwerk des Privacy Shield, das die Europäische Kommission als Ersatz für den vom EuGH für nichtig erklärten „Sicheren Hafen“ (Safe Harbor) beschlossen hat, in jährlichem Rhythmus vorgesehen. Der Hessische Datenschutzbeauftragte war intensiv an der ersten jährlichen Überprüfung des Privacy Shield beteiligt. Zusammen mit sieben weiteren Vertretern der Artikel 29-Datenschutzgruppe bildete eine Mitarbeiterin des Hessischen Datenschutzbeauftragten die Delegation der Artikel 29-Datenschutzgruppe und repräsentierte damit die europäischen Datenschutzaufsichtsbehörden. Diese Delegation führte zusammen mit Vertretern der Europäischen Kommission sowie Vertretern verschiedener US-Behörden wie dem US-Handelsministerium die erste jährliche Überprüfung des Privacy Shield durch.

Die Existenz tragfähiger Mechanismen, die es Unternehmen ermöglichen, personenbezogene Daten in die USA zu transferieren, sind für die digitale Wirtschaft von enormer Bedeutung. Die Artikel 29-Datenschutzgruppe hatte jedoch schon bei der Entstehung des Privacy Shield Zweifel daran geäußert, ob die von der Europäischen Kommission gemeinsam mit den USA entwickelten Mechanismen zum Schutz personenbezogener Daten den hohen Anforderungen, die der EuGH formuliert hat, genügen. Auch die Europäische Kommission hatte im Vorfeld betont, dass im Regelwerk des Privacy Shield vorgesehen ist, dass sie den Privacy Shield aussetzt oder aufhebt, wenn nicht nachgewiesen werden kann, dass der Privacy Shield einen dem Schutzniveau in der EU gleichwertigen Schutz bietet.

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

Die erste Überprüfung war daher eine auf beiden Seiten des Atlantik ernst genommene Aufgabe, was sich auch daran zeigte, dass das Weiße Haus in einer Pressemitteilung den Willen der USA bekräftigte, im Rahmen der Prüfung nachzuweisen, dass der Privacy Shield einen starken Schutz für die Daten, die auf seiner Grundlage in die USA transferiert werden, bietet: https://www.whitehouse.gov/briefings-statements/statement-press-secretary-eu-u-s-privacy-shield/. Um die Bedeutung der Prüfung zu unterstreichen, eröffneten Kommissarin Věra Jourová und der US-Handelsminister Wilbur Ross persönlich die Prüfung.

Im Rahmen der Überprüfung wurden Verbände und Nichtregierungsorganisationen in den Vereinigten Staaten von Amerika angehört und um Informationen zu ihren Erfahrungen mit dem Privacy Shield gebeten. Außerdem wurden die Erfahrungen der europäischen Datenschutz-Aufsichtsbehörden, Fragen der praktischen Umsetzung des Privacy Shield sowie bereits bei der Verabschiedung des Privacy Shield durch die Europäische Kommission im Jahre 2016 von den Datenschutz-Aufsichtsbehörden geäußerte Kritikpunkte zusammengetragen und gemeinsam mit den US-Behörden eine Tagesordnung für ein zweitägiges Treffen in Washington D.C. erstellt.

Bei der Überprüfung vor Ort wurden zwei Themenfelder intensiv untersucht: Zum einen die sog. kommerziellen Aspekte, das bedeutet im Wesentlichen die Bestimmungen über die Zertifizierungskriterien sowie das Verfahren der Zertifizierung selbst. Zum anderen Fragen rund um staatliche Zugriffe auf die unter dem Privacy Shield in die USA exportierte Daten und Rechtsschutzmöglichkeiten Betroffener hiergegen.

Die Erkenntnisse der Delegation der Artikel 29-Datenschutzgruppe wurden in einem ausführlichen Bericht zusammengefasst. Dieser wurde von der Artikel 29-Datenschutzgruppe bewertet. Die gezogenen Schlussfolgerungen sind zusammen mit dem Bericht unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782 veröffentlicht.

In beiden untersuchten Themenfeldern sieht die Artikel 29-Datenschutzgruppe erheblichen Nachbesserungsbedarf:

Sie fordert die US-Behörden dazu auf, Privacy Shield zertifizierten US-Unternehmen generell mehr Leitlinien an die Hand zu geben, um die Anforderungen, die zum Beispiel an die Weiterübermittlung von Daten an Dritte zu stellen sind, zu verdeutlichen.

Im Zusammenhang mit staatlichen Zugriffen auf Daten, die auf der Grundlage des Privacy Shield übermittelt werden, hatte sich die Europäische Kommission mit den USA unter anderem

darauf verständigt, eine unabhängige Ombudsperson zu benennen. Diese soll Betroffenen die Möglichkeit eröffnen, die Rechtmäßigkeit von staatlichen Zugriffen auf personenbezogene Daten von einer unabhängigen Stelle überprüfen zu lassen. Bislang ist allerdings weder eine Ombudsperson benannt worden, noch war es im Rahmen der Prüfung möglich, sich ein konkretes Bild von der Arbeitsweise und den Befugnissen der Ombudsperson zu machen, da diese Informationen als vertraulich eingestuft waren. Auch die fehlende Benennung von Mitgliedern des Privacy and Civil Liberties Oversight Board (PCLOB), eines Gremiums, das dafür sorgen soll, dass bei Regelungen zur Bekämpfung von Terrorismus die Privatsphäre (privacy) und bürgerliche Freiheitsrechte (civil liberties) angemessen Berücksichtigung finden, wird dringend angemahnt.

Die Artikel 29-Datenschutzgruppe hat die Kommission und die zuständigen US-Behörden dazu aufgefordert, sämtliche geäußerten Bedenken in einen Aktionsplan aufzunehmen und spätestens bis zur nächsten jährlichen Überprüfung auszuräumen. Die Benennung von Ombudsperson und PCLOB-Mitgliedern soll bereits zum 25.05.2018 erfolgen. Um ihren Forderungen Nachdruck zu verleihen, hat die Artikel 29-Datenschutzgruppe angekündigt, dass ihre Mitglieder geeignete Maßnahmen – einschließlich der Klageerhebung – gegen die Angemessenheitsentscheidung über den Privacy Shield vor den nationalen Gerichten ergreifen werden.

Nach wie vor besteht in dem Themenfeld internationale Datentransfers große Unsicherheit. Ausgehend von den Enthüllungen Edward Snowdens und der Nichtig-Erklärung der sog. Safe Harbor-Entscheidung der Europäischen Kommission sowie weiterer Rechtsprechung europäischer Gerichte sind derzeit Verfahren vor europäischen Gerichten anhängig, mit denen auch die Wirksamkeit der Standardvertragsklauseln und des Privacy Shields in Frage gestellt werden.

4.2
Ziele und Aufgaben der IT Task Force im Jahr 2017

Wie im 45. Tätigkeitsbericht dargestellt, hat die IT Task Force (ITTF) ihre Arbeit auf der Basis der Arbeitspläne der Artikel 29-Gruppe für das Jahr 2016, wie auch für das folgende Jahr 2017 durchgeführt. Die Aufgabe der ITTF ist, eine geeignete IT Infrastruktur bis zum 25.05.2018 für die kooperativen Verfahren und das Kohärenzverfahren bereitzustellen. Entsprechend ihres Mandats hat die ITTF in einem aufwändigen Prozess die Artikel 29-Gruppe in ihrer Entscheidung unterstützt. Dabei wurde das am einfachsten zu erweiternde International Market Information-System (kurz: IMI-System) ausgewählt.

In dieser IT Task Force vertritt eine Mitarbeiterin von mir die Datenschutzaufsichtsbehörden der Länder für Deutschland[1].

Die Artikel 29-Gruppe hat sich aufgrund der Vorarbeiten der IT Task Force für den Einsatz des IMI-Systems für die Dauer von zwei Jahren als Pilot entschieden[2]. Dabei wurde die Prüfung zusätzlicher Entwicklungsaufwände („gap analysis“) durch DG GROW – einem „Directorates-General Service“ der EU Kommission – berücksichtigt.

Das IMI-System basiert auf einer Struktur von Formularen, die miteinander verbunden bzw. verlinkt werden können, so dass sich für die benötigten IT-Prozesse ein Workflow herstellen lässt. Jedem Formular lassen sich weitere eigene Dateien in üblichen Formaten anhängen, wie pdf-, Word- oder Bild-Dateien in ebenso gängigen Formaten. Die ausgefüllten Formulare eines Workflows werden im IMI-System gespeichert. Aufgrund von standardisierten Attributierungen (in Metadaten) kann nach einzelnen Vorgängen (Cases) gesucht werden. Ein oder mehrere Formulare eines Workflows können zu jeder Zeit in eine pdf-Datei transformiert werden; sie können auf diese Weise in ein eigenes Content-Management-/Dokumenten-Archiv-System übertragen werden[3]. Eine Alternative für bereits erfasste Daten aus Formularen des IMI-Systems ist, jedes Formular über eine csv-Schnittstelle zu exportieren. Eine vergleichbare import-Funktion zum IMI-System ist für die Aufsichtsbehörden erst nach Mai 2018 vorgesehen.

Einige Aspekte sollen hervorgehoben werden:

– Die bestehende IMI-Verordnung sieht die Unterstützung von kooperativen Verfahren vor. Eine entsprechende Anpassung der Verordnung für das Kohärenzverfahren kann laut Aussage von DG Justice während der Laufzeit des Piloten erfolgen.
– Das IMI-System ist für den Einsatz in föderativen Staaten vorgesehen, so dass alle zuständigen Datenschutzaufsichtsbehörden gleichberechtigten Zugang und Zugriff erhalten.
– Für die Anwendung der Client-Server-Architektur mit dem dazugehörigen Web-Client des IMI-Systems spricht, dass eine Vielzahl von IT-Sicherheitsstandards bereits implementiert ist; so ist z. B. die sichere, wie auch verschlüsselte und eindeutig zuzuordnende Übertra-

[1] Teilnehmer sind unter der Leitung der „IT Policy“-Abteilung beim Europäischen Datenschutzbeauftragten: Herr Achim Klabunde und mindestens drei Personen aus seinem Team, die Mitgliedsstaaten FR, IT, GB (Mai 2016 bis April 2017), für Deutschland Hessen (HE) und seit 01.02.2017 auch ein Vertreter der BfDI.

[2] Vgl. Protokoll des Plenums am 03. und 04.10.2017

[3] Mit dieser Konstruktion ist es möglich zu entscheiden, welche Unterlagen bzw. Dateien in das innewohnende Repository des IMI-Systems überführt werden (und welche nicht). Die Dokumentenverwaltungssysteme bei den Ländern bzw. Aufsichtsbehörden bleiben in ihrer Funktionsweise unberührt.

gung von Daten und Dateien gewährleistet. Die Speicherung der Formulare und Dokumente bzw. angehängten Dateien erfolgt ebenfalls in einer geschützten Umgebung der EU[4].

Die Basis-Nutzung des IMI-Systems mit seinen bis jetzt geplanten, datenschutzrechtlichen Erweiterungen ist für jede Aufsichtsbehörde in Bezug auf zu erwerbende Lizenzen oder zusätzlichen Speicherplatz kostenfrei. In geringem Umfang können Personalkosten entstehen, weil Zugang- und Zugriffsberechtigungen durch die Systemadministratoren der jeweiligen Aufsichtsbehörde über eine Web-Oberfläche im IMI-System zu pflegen sind. Die Finanzierung des Entwicklungsaufwands für eine vergleichbare import-Funktion zum IMI-System für die Aufsichtsbehörden kann zu Kosten führen.

Die Weiterentwicklung, d. h. die notwendige Anpassung, sowie die Wartung des IMI-Systems wird durch DG GROW übernommen. Die Zentrale von DG GROW liegt unweit des heutigen Büros des Europäischen Datenschutzbeauftragten und wird sich in unmittelbarer Nähe des zukünftigen Sekretariats des Europäischen Datenschutzausschusses (EDSA) befinden. Die Nutzung durch die Datenschutzaufsichtsbehörden wird im laufenden Betrieb ab 26.05.2018 durch das Sekretariat des EDSA betreut.

Gemäß Beschluss der Artikel 29-Gruppe vom 03.10.2017 setzt die IT Task Force ihre Arbeit mindestens bis zum 25.05.2018 fort. Bis dahin wird die IT Task Force die Bereitstellung des angepassten IMI-Systems für die Nutzung durch die Datenschutzaufsichtsbehörden aller Mitgliedsstaaten in der EU begleiten und kontrollieren. Ein besonderes Augenmerk wird dabei auf dem ersten Betrieb in einer intensiven Test- und Einführungsphase liegen, die von Januar bis März 2018 stattfinden soll.

[4] Ein externer Cloud-Speicherdienst wird nicht benötigt.

5. Polizei, Justiz, Verfassungsschutz, Ordnungswidrigkeitenverfahren

5.1
Beteiligung privater Dienstleister im Rahmen der Verkehrsüberwachung

Der Beschluss des OLG Frankfurt vom 26.04.2017 hat mit strengen Anforderungen an den Einsatz moderner Verkehrsüberwachungseinrichtungen zu erheblichen Veränderungen in der Überwachungspraxis geführt und insbesondere die dabei mögliche Unterstützung durch private Dienstleister begrenzt.

Schon seit einigen Jahren kommen durch die örtlichen Ordnungsbehörden zur Geschwindigkeitskontrolle immer öfter nicht mehr klassische „Blitzer“, sondern digitale Geräte zum Einsatz. Damit werden nicht mehr Fotos im herkömmlichen Sinne, sondern Messungen und „Beweisfotos“ in digitaler Form erstellt.

Nicht immer stehen die verwendeten digitalen Geräte im Eigentum der Kommunen. Zum Teil werden diese nur gemietet, mobile Anlagen auch nur tageweise von Dienstleistern zur Verfügung gestellt. Auch bei der Verarbeitung der mit diesen Geräten erfassten Daten gibt es unterschiedliche Ausgestaltungen der Unterstützung der Verwaltungsbehörden.

Die Zulässigkeit der Einbeziehung privater Dienstleister im Rahmen der Verkehrsüberwachung richtet sich nach § 4 HDSG. Eine solche Unterstützung ist grundsätzlich als Auftragsdatenverarbeitung zulässig, weil dabei die Verantwortung der Kommune für die hoheitliche Tätigkeit nicht verletzt wird.

§ 4 HDSG

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

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

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

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

Dies war daher auch in einem Erlass des Hessischen Innenministers zur „Verkehrsüberwachung durch örtliche Ordnungsbehörden“ vom 05.02.2015 (StAnz. 2015, S. 183) ausdrücklich bestätigt. Da es in der Praxis allerdings zu verschiedenen Verstößen gegen die Wahrung der Verantwortung für die hoheitliche Tätigkeit kam, hat das Oberlandesgericht Frankfurt am Main mit Beschluss vom 26.04.2017 (Az: 2 Ss-Owi 295/17) enge Rahmenbedingungen für die Beteiligung Privater formuliert. Dies veranlasste sowohl einige Ordnungsbehörden als auch die zentrale Bußgeldstelle beim Regierungspräsidium in Kassel mich um eine Einschätzung der vorhandenen Vertragskonstellationen bzw. der Möglichkeiten der zukünftigen Beteiligung privater Dienstleister zu bitten.

Da es mir – nicht zuletzt aus Kapazitätsgründen – nicht möglich ist, umfassend alle unterschiedlichen Vertragsgestaltungen bzw. technischen Ausgestaltungen zu beurteilen, habe ich zunächst ausgehend von der Entscheidung des Oberlandesgerichts die Anforderungen an eine rechtskonforme Nutzung der Messanlagen bzw. Auswertung der Messdaten skizziert.

Alle Geschwindigkeitsmessgeräte bedürfen einer Bauartzulassung der Physikalisch-Technischen Bundesanstalt (PTB). Diese umfasst auch die für den Einsatz erforderliche Software. Damit ist bei Einhaltung der jeweiligen Vorgaben zum Aufbau des Gerätes, der Gestaltung der Messstrecke etc. grundsätzlich die Richtigkeit der Messung und damit auch die Verwendung der gewonnenen Daten als Beweismittel gewährleistet.

Da es sich bei der Ahndung von Verkehrsverstößen um eine hoheitliche Tätigkeit handelt, ist für die Erstellung und jegliche Verarbeitung der Beweismittel sicherzustellen, dass die hoheitliche Verantwortung gewährleistet ist. Das gilt zunächst für die Auswertung der Messdaten und Beweisbilder als Grundlage der Entscheidung, ein Ordnungswidrigkeitsverfahren einzuleiten. Aber auch die technische Ausgestaltung des Messvorgangs und im Anschluss des Auslesens und Aufbereitens der so gewonnenen Daten in ein lesbares Format muss eine Manipulationsmöglichkeit durch Dritte ausschließen.

Das Oberlandesgericht hat dazu in seiner Entscheidung drei Prämissen benannt:

– Die Ordnungsbehörde muss Herrin des Messgerätes sein.
– Die Ordnungsbehörde muss Herrin des durch die Messanlage gewonnenen Beweismittels sein (Garantie der Authentizität der Messdaten).
– Die Ordnungsbehörde muss die Umwandlung und Auswertung des Beweismittels selbst durchführen (Garantie der Rückführbarkeit des Messbildes und der Messdaten auf die digitalen Messrohdaten bzw. Falldateien).

Die vom OLG beschriebenen Anforderungen führen zu erheblichen Konsequenzen für die Praxis und letztlich zu Einschränkungen der Möglichkeiten in der Unterstützung durch private Dienstleister. Dies betrifft

1. Anforderung auf Sicherung der Rohdaten (Falldateien), um (nachträgliche) Kontrollen zu ermöglichen, die Richtigkeit der Messdaten und Beweisfotos nachträglich zu überprüfen
   – Aussage des OLG:
     „...muss sie (die Ordnungsbehörde) im ununterbrochenen Besitz dieser digitalen Messrohdaten bzw. Falldateien sein.“
   – Konsequenzen für die Praxis:
     – Der Dienstleister/Vertreiber darf zu keinem Zeitpunkt dergestalt Zugriff auf die Rohdaten haben, dass er Änderungen vornehmen oder Daten löschen kann.
     – Die Auswertung erfolgt i. d. R. anhand einer Kopie der Rohdaten, damit diese für eine spätere Verifikation in der Originalform vorliegen.

2. Anforderungen zur „Entnahme“ der Rohdaten (Auslesen, Online-Zugriff etc.)
   - Aussage des OLG:
     „...die Gewinnung des Beweismittels (i. d. R. die digitalen Messrohdaten bzw. Falldateien ...) muss durch die Ordnungsbehörde selbst erfolgen.“
   - Konsequenzen für die Praxis:
     - Sicher ist diese Anforderung erfüllbar, wenn die Daten vor Ort mittels eines Datenträgers aus der Messanlage ausgelesen werden und dies durch Ordnungsamtsmitarbeiter erfolgt.
     - Ein Fernzugriff ist möglich, soweit technisch sichergestellt ist, dass nur ein Mitarbeiter der Ordnungsbehörde auf die in der Messanlage gespeicherten Beweismittel zugreifen kann. Dies kann z. B. durch eine zertifikatsbasierte Identifizierung und Authentifizierung sowie eine verschlüsselte Datenübertragung erfolgen.
     - Ein „Auslesen“ durch den Dienstleister und ein Zurverfügungstellen in einer Cloud oder auf einem Web-Portal ist ausgeschlossen, da damit der durchgehende Besitz der Verwaltungsbehörde nicht sichergestellt ist.

3. Anforderungen an die Auswertung der gewonnenen Daten
   - Aussagen des OLG:
     - „Primäre Beweismittel sind die in Messbild und Messdaten umgewandelten Falldateien. Die Umwandlung dieser digitalen Dateien in eine lesbare und damit auswertbare und gerichtsverwertbare Form durch von der PTB zugelassene Programme ist hoheitliche Kernaufgabe der Ordnungsbehörde.
     - Für die Auswertung der Messdaten ist die Hinzuziehung privater Dienstleister kraft Gesetz ausgeschlossen.“
   - Konsequenzen für die Praxis:
     - Die Auswertung mit den von der PTB zugelassenen Programmen – auch eine Vorselektion im Sinne von gut verwendbare Bilder, gar nicht verwendbare Bilder sowie ggf. zu bearbeitende Bilder – muss immer komplett durch Mitarbeiter der Ordnungsbehörde geschehen.
     - Die Verwendung der zugelassenen Programme muss auf Rechnern erfolgen, auf die der Dienstleister/Vertreiber der Messanlage keinen Zugriff hat. Der Vertreiber der Messanlage kann nur insoweit unterstützend/beratend zur Seite stehen, soweit bei Problemen ein Support ohne Zugriff auf die Beweismittel und Auswertungen möglich ist.
     - Die Wartung der Geräte kann durch andere Dienstleister erfolgen.

Die vom OLG formulierte Anforderung, dass die Ordnungsbehörde Herrin des Messgerätes sein muss, schließt ein Mieten einer Anlage nicht aus, solange der Betrieb den o. g. Anforderungen entspricht. Auch die Entscheidung, wo ein Messgerät aufgestellt wird, muss allein durch die Ordnungsbehörde getroffen werden.

Gerade für kleinere Kommunen gibt es das Angebot eines Dienstleisters, nicht nur die mobile Überwachungsanlage zu mieten, sondern auch einen Rechner mit der notwendigen Auswertesoftware zur Verfügung zu stellen. Dazu befindet sich in dem Messfahrzeug auch ein Laptop, auf dem sich die Auswertesoftware befindet, mit deren Hilfe die Daten vor Ort so aufbereitet werden können, dass im Anschluss durch die Ordnungsbehörde ein Transfer direkt in die zur Durchführung der Bußgeldverfahren verwendete Software möglich ist. Dies hat den Vorteil für die einzelnen Ordnungsbehörden, dass die zusätzlichen Lizenzgebühren für die Software nur einmalig und nicht für jede Behörde getrennt anfallen.

Dies halte ich unter der Voraussetzung für zulässig, dass der Rechner so konfiguriert wird, dass weder eine Manipulation des Programms und damit auch der zu verarbeitenden Daten durch den Dienstleister möglich ist, noch ein Zugriff auf Daten eines Vertragspartners durch einen anderen Mieter des Messfahrzeuges oder den Dienstleister erfolgen kann.

5.2
Kontrolle der Rechtsextremismus-Datei

Bei meiner Überprüfung der Rechtsextremismus-Datei stellte ich fest, dass Mängel im Rahmen der notwendigen Dokumentation bestanden. Nicht in allen Fällen war es möglich, die Gründe für die Speicherung nachzuvollziehen.

Rechtliche Rahmenbedingungen

Die Rechtsextremismus-Datei soll den Sicherheitsbehörden bei der Bekämpfung von rechtsextremistischen Gewalttaten dienen. Das entsprechende Gesetz hierzu, das Rechtsextremismus-Datei-Gesetz (RED-G), sieht die Errichtung dieser Datei vor, in welcher die Daten von Personen mit rechtsextremistischem Hintergrund gespeichert werden. Weiterhin hat der Gesetzgeber in § 11 Abs. 1 S. 2 und Abs. 2 RED-G normiert, dass die Datei alle zwei Jahre datenschutzrechtlich überprüft werden muss. Zuständig für die Kontrolle der durch die Behörden

der einzelnen Länder eingegebenen personenbezogenen Daten sind die Datenschutzbeauftragten der Länder.

In Hessen stellen sowohl die Polizei durch das Landeskriminalamt (LKA) als auch das Landesamt für Verfassungsschutz (LfV) Daten in die Datei ein, so dass ich bei beiden Institutionen die Voraussetzungen für eine Speicherung überprüft habe. Bei der datenschutzrechtlichen Überprüfung habe ich vor allem kontrolliert, ob die gesetzlichen Voraussetzungen für die Speicherung erfüllt waren und diese nachvollziehbar dokumentiert worden ist.

Nach § 2 Nr. 1 RED-G müssen die Daten von Personen in der RED gespeichert werden, wenn sie einer rechtsextremistischen Vereinigung angehören oder diese unterstützen oder eine rechtsextremistische Gewalttat begangen haben. § 2 Nr. 2 RED-G sieht eine Speicherung vor, wenn Personen rechtsextremistische Bestrebungen verfolgen und in diesem Zusammenhang zur Gewalt aufrufen.

§ 2 Nr. 1 und 2 RED-G

Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Absatz 1 in der Datei nach § 1 zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, dass die Daten sich beziehen auf

1. Personen,
   a) bei denen Tatsachen die Annahme rechtfertigen, dass sie einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs mit rechtsextremistischem Hintergrund angehören oder diese unterstützen,
   b) die als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte oder rechtskräftig Verurteilte sind;

2. Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und in Verbindung damit zur Gewalt aufrufen, die Anwendung von rechtsextremistisch begründeter Gewalt als Mittel zur Durchsetzung politischer Belange unterstützen, vorbereiten oder durch ihre Tätigkeiten vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderlichen waffenrechtlichen Berechtigungen, Kriegswaffen oder Explosivstoffe aufgefunden wurden, oder

….

Ergebnis der Prüfung

1. Prüfung beim Landesamt für Verfassungsschutz (LfV)

Beim LfV habe ich alle gespeicherten Fälle anhand der Akten auf die Rechtmäßigkeit der Speicherung hin überprüft. Insgesamt war festzustellen, dass grundsätzlich das Vorliegen der Speichervoraussetzungen bejaht werden konnte, problematisch war jedoch die Dokumentation. So gab es in einigen Fällen nur kurze handschriftliche Vermerke auf anderen Dokumenten, aus denen nicht hervorging, weshalb die jeweilige Person als rechtsextrem eingestuft wurde und weshalb davon ausgegangen wurde, dass zusätzlich die Anforderungen des § 2 RED-G erfüllt sein sollten. In anderen Fällen war eine zusammenhängende und schlüssige Ordnung der Unterlagen in den Akten nicht ersichtlich, so dass nicht nachvollzogen werden konnte, welcher Mitarbeiter sich aus welchem Grund für die Speicherung der Person entschieden hat.

Das Landesamt für Verfassungsschutz hat als Konsequenz aus meiner Prüfung die Erstellung fehlender Speichervermerke veranlasst und den Aufbau der Akten geändert, so dass künftig die Entscheidung und die Gründe leichter auffindbar sein werden. Weiterhin hat das LfV angekündigt, jährliche Kontrollen hinsichtlich der Speichervoraussetzungen durch einen RED-Verantwortlichen durchzuführen und diese Kontrolle zu dokumentieren.

2. Prüfung beim Hessischen Landeskriminalamt (LKA)

Die Einstellung der Daten in die RED erfolgt durch das Landeskriminalamt (LKA), das auch die Entscheidung über die Erfassung in der Datei trifft. Grundlage ist dabei in der Regel die Information durch die sachbearbeitenden Dienststellen. Für eine eventuelle Speicherung in der RED werden Datenblätter angelegt und dem zuständigen Sachgebiet des LKA zugeleitet und dort ausgewertet. Bei einer Speicherung wird das Datenblatt ausgedruckt und vorgehalten. Die Kriminalakte bleibt jedoch bei den Polizeidienststellen und konnte daher bei meiner Kontrolle nicht mit herangezogen werden.

Nach stichprobenartiger Durchsicht gespeicherter Vorgänge gab es Fälle, bei denen die Relevanz für eine solche Datei nicht erkennbar war. So gab es etwa Speicherungen über eine Schlägerei unter mehreren Personen, bei denen jedoch kein rechtsextremer Hintergrund allein aus den beim LKA vorhandenen Unterlagen zu erkennen war. Weiterhin gab es Fälle, bei welchen die betroffene Person verfassungswidrige Kennzeichen getragen hatte oder rechtsextreme Parolen gegenüber Polizisten gerufen hatte, die Voraussetzungen des § 2 Nr. 2 RED-G jedoch nach der Aktenlage nicht erfüllt waren, da weder ein Aufruf zur Gewalt noch die Akzeptanz von Gewalt zur Durchsetzung politischer Belange belegt werden konnten.

Nach Auskunft des LKA wird zum Teil auch in den sachbearbeitenden Dienststellen nachgefragt, bevor eine Entscheidung über die Speicherung erfolgt. Diese entscheidungsrelevanten Hintergrundinformationen aus den Kriminalakten waren jedoch nicht in den Unterlagen vermerkt und konnten daher bei der Kontrolle auch nicht nachvollzogen werden.

Bei der Prüfung sind ebenfalls Fragen zur Löschung der Daten und zu Mitzieheffekten aufgefallen, welche durch Fälle ausgelöst wurden, bei denen zunächst kein Bezug zur politisch motivierten Kriminalität ersichtlich war. So fanden sich Fälle, bei denen die Aussonderungsprüffrist abgelaufen war, jedoch in POLAS andere Straftaten in der Zwischenzeit eingetragen waren, die keinen rechtsextremen Bezug hatten, aufgrund derer sich jedoch die Speicherfristen in der RED entsprechend verlängerten. Dass diese Taten die Speicherfristen der RED auch ohne rechtsextremen Zusammenhang beeinflussen, halte ich für datenschutzrechtlich nicht zulässig. Weiterhin gibt es Strafverfahren, die eingestellt wurden und die Einstellung der Polizei auch entsprechend mitgeteilt wurde, so dass die Daten in POLAS gelöscht werden konnten. Nicht sichergestellt erschien es mir jedoch, dass auch das LKA eine entsprechende Mitteilung erhält, um auch die Löschung der Daten in der RED zu veranlassen.

Ich habe dem LKA meine Feststellungen mitgeteilt und um eine Stellungnahme gebeten, die mir allerdings bis zum Redaktionsschluss noch nicht vorlag.

5.3
Dürfen Behörden privat erstellte, digitale Fotoaufnahmen als Beweismittel zulassen?

Die Frage, ob Behörden Fotoaufnahmen Dritter als Beweismittel anerkennen dürfen, lässt sich nicht pauschal beantworten. Maßgeblich sind die Umstände des Einzelfalls.

Der Anlass

Ein Bürger nimmt Anstoß daran, dass entgegen einer kommunalen Satzung Wasservögel im städtischen Gebiet gefüttert werden, und dokumentiert das ordnungswidrige Verhalten mit Fotos, die er mit seinem Smartphone fertigt. Ein Anwohner fotografiert einen Falschparker, der verbotswidrig die Einfahrt zu seinem Grundstück blockiert. Die jeweiligen Beweisbilder werden der Verfolgungsbehörde als Beweismittel zugänglich gemacht.

Nicht selten gelangen derartige Sachverhalte zur rechtlichen Beurteilung an meine Dienststelle, wobei regelmäßig die Betroffenen der dokumentierten Ordnungswidrigkeit sich in ihren Persönlichkeitsrechten verletzt fühlen.

Rechtliche Bewertung

Das digitale Fotografieren stellt eine Datenerhebung im Sinne von § 3 Abs. 3 BDSG und eine Datenverarbeitung im Sinne von § 3 Abs. 4 BDSG dar. Da sich die Vorschrift des § 6b BDSG nur auf die Beobachtung, also eine auf eine bestimmte oder unbestimmte Dauer ausgerichtete Aufzeichnung, bezieht, kann diese beim Fertigen von digitalen Fotos nicht zur Anwendung kommen.

Auch bei privat erstellten Fotos handelt sich um die Verarbeitung personenbezogener Daten, wenn beispielsweise eine Person aufgrund einer Gesichtsaufnahme individualisiert werden kann oder ein amtliches Kfz-Kennzeichen im Zusammenhang mit Zeit und Ort eine Einzelangabe über persönliche oder sachliche Verhältnisse einer Person darstellt. Beweisaufnahmen von ordnungswidrigen oder strafrechtlich relevanten Verhältnissen oder Zuständen ohne Personenbezug bzw. Beziehbarkeit, beispielsweise ein Foto von rechtswidrig abgelagertem Müll, unterliegen dagegen nicht den Vorschriften des BDSG.

Das BDSG sieht für die Datenverarbeitung jedoch in § 27 Abs. 1 Satz 2 BDSG eine Ausnahme insbesondere dann, wenn die Verarbeitung von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird. Das Beweisbild, welches alleine zum Zweck der Weitergabe und der beweiskräftigen Dokumentation an eine Verfolgungsbehörde gefertigt wurde, kann von dieser Ausnahmeregelung des § 27 Abs. 1 Satz 2 BDSG grundsätzlich nicht gedeckt sein.

Eine Dokumentation durch eine Datenerhebung mittels digitaler Bilder kann deshalb berechtigt sein, soweit dies dem Schutz eigener subjektiver Rechte oder der Verfolgung einer entsprechenden Rechtsverletzung dient.

Bei Betrachtung der beiden Beispielfälle wird das Abgrenzungsmerkmal offensichtlich erkennbar. Während die Person, die die Fütterung der Wasservögel dokumentiert, von der Ordnungswidrigkeit nicht unmittelbar beeinträchtigt wird, wird die Person, deren Grundstückseinfahrt blockiert wird, tatsächlich in der Nutzung dieser Einfahrt beeinträchtigt.

Unabhängig davon, ob im Einzelfall das Erstellen der Aufnahme berechtigt war, steht es im Ermessen der Verwaltungsbehörde, ob sie das Ereignis im Rahmen eines Ordnungswidrigkeitsverfahrens ahndet. Es ist auch allein ihre Entscheidung, ob sie dazu die privat erstellten Beweisbilder heranzieht. Ein Beweisverwertungsverbot für die Fälle, in denen das Anfertigen des Fotos nicht gerechtfertigt war, gibt es nicht.

5.4
Lichtbildabgleich bei der Verfolgung von Verkehrsordnungswidrigkeiten

Im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten ist es häufig geboten, das Beweisfoto mit dem Foto im Personalausweis- bzw. Passregister abzugleichen. Ein derartiger Abgleich ist zulässig.

Ich werde immer wieder mit Beschwerden konfrontiert, dass die Bußgeldbehörde zur Identifizierung des Fahrers auf Fotos aus dem Pass- bzw. Personalausweisregister zurückgreift.

Sowohl das Personalausweisgesetz als auch das Passgesetz enthalten Regelungen, die die Übermittlung von Daten an andere Behörden regeln und damit einen Lichtbildabgleich durch die Verfolgungsbehörde ermöglichen.

§ 24 Abs. 2 Nr. 3 PAuswG

Die Personalausweisbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln, wenn

...

3. die ersuchende Behörde die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erheben kann oder wenn nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.

§ 22 Abs. 2 Nr. 3 PaßG

Die Paßbehörden dürfen anderen Behörden auf deren Ersuchen Daten aus dem Paßregister übermitteln. Voraussetzung ist, daß

...

3. die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muß.

Zur Anwendung kommt hier die Vorschrift des § 24 Abs. 2 Nr. 3 PAuswG bzw. § 22 Abs. 2 Nr. 3 PaßG. In der Praxis ist vorwiegend die dreimonatige Verjährungsfrist und der damit einhergehende Zeitdruck für die Verfolgungsbehörde Hintergrund für die Durchführung eines Lichtbildabgleichs unter Heranziehung eines Lichtbildes aus Personalausweis- bzw. Passregister, soweit zunächst ein Anhörungsversuch gemäß § 55 OWiG erfolglos blieb.

Die näheren Rahmenbedingungen sind im Erlass des HMdIS formuliert (StAnz. 2015, S. 182, Ziff. 3.2). Demnach ist bereits im Rahmen der Anhörung auf einen möglichen Lichtbildabgleich hinzuweisen. Soweit erforderlich, d. h. nachdem andere Ermittlungsmaßnahmen erfolglos blieben und die Verjährung droht, richtet die Verfolgungsbehörde ein Ersuchen an die für die Halteranschrift zuständige Ordnungsbehörde, das aktuellste Lichtbild aus dem Personalausweis- bzw. Passregister zu übermitteln. Ein solches Ersuchen darf nur von Bediensteten gestellt werden, die vom jeweiligen Behördenleiter dazu besonders ermächtigt sind.

Die Praxis der Fahrerermittlung mittels eines Lichtbildabgleichs stellt nach meiner Einschätzung in der Regel eine weniger belastende Maßnahme als das unmittelbare Auftreten und Ermitteln von Ordnungs- oder Vollzugspolizeibeamten an der Halteranschrift dar. Deshalb stufe ich die im Erlass beschriebene Vorgehensweise als zulässig ein.

5.5
Pilotprojekt zur Section-Control

Das Pilotprojekt „Section-Control“, bei dem eine Durchgangsstraße mit einem System überwacht werden soll, das die Durchschnittsgeschwindigkeit durchfahrender Fahrzeuge misst, entspricht den datenschutzrechtlichen Anforderungen.

Der Anlass

Eine hessische Kommune hat mir ein Projekt zur Section-Control vorgestellt und mich um eine Einschätzung gebeten, ob dieses Projekt im Rahmen der derzeitigen gesetzlichen Regelungen durchgeführt werden kann. Vorgesehen ist, in einem Ortsteil eine Durchgangsstraße zu überwachen, für die eine Geschwindigkeitsbeschränkung von 30 km/h besteht. Da diese Straße auch als Ausweichstrecke für eine nahgelegene Autobahn genutzt wird, gibt es hier ein erhebliches Verkehrsaufkommen.

Die besondere Problematik beim Einsatz der sog. Section-Control besteht darin, dass zunächst alle in den überwachten Streckenabschnitt einfahrenden Fahrzeuge erfasst werden müssen, unabhängig davon, ob sie gegen die vorgeschriebene Höchstgeschwindigkeit verstoßen. Die Erfassung erfolgt vergleichbar der Geschwindigkeitsüberwachung, d. h. es werden zunächst die Kennzeichen der Fahrzeuge erfasst und bei einem festgestellten Geschwindigkeitsverstoß Fotos erstellt. Im Rahmen der Ortsdurchfahrt können auch Fahrzeuge erfasst werden, die gar nicht die gesamte Strecke befahren, sondern vorher abbiegen. Somit fallen in einer nicht unerheblichen Anzahl Daten zu Fahrzeugen und Fahrern an, die sich regelkonform verhalten. Da erst zu einem späteren Zeitpunkt festgestellt wird, ob ein Regelverstoß vorliegt, könnte man dies auch als Datenerhebung auf Vorrat bezeichnen. Denn die Tatsache und der Zeitpunkt des Einfahrens in die Messstrecke ist nur für solche Fahrzeuge relevant, für die am Ende der Messtrecke ein Geschwindigkeitsverstoß festgestellt wird.

Technische Beschreibung

Im Gegensatz zu einer stationären Geschwindigkeitsüberwachung sind für die Überwachung der Durchschnittsgeschwindigkeit eines Straßenabschnitts mehrere Komponenten erforderlich:

– Fahrzeugerfassung beim Einfahren in den Streckenabschnitt (Einfahrstation)
– Fahrzeugerfassung beim Verlassen des Streckenabschnitts (Ausfahrstation)
– Mess- und Erfassungseinheit nach der Ausfahrstation (bei bidirektionaler Überwachung sind zwei Mess- und Erfassungseinheiten erforderlich)

1. Vor der Inbetriebnahme werden die Stationen exakt vermessen, geeicht und versiegelt. Dabei wird auch die Mindestdurchfahrtzeit bei Einhaltung der Höchstgeschwindigkeit (Referenzzeit) gespeichert.

2. Sobald ein Fahrzeug die Einfahrstation passiert, wird neben dem Kennzeichen der exakte Zeitpunkt der Durchfahrt festgehalten. Das Kennzeichen wird über ein Heckbild erfasst, so dass weitestgehend ausgeschlossen ist, dass auf dem Bild auch Fahrzeuginsassen erkennbar sind.
   Dieser Datensatz wird per Funk oder Kabel verschlüsselt zur Ausfahrstation übertragen.

3. Passiert ein Fahrzeug die Ausfahrstation, werden ebenfalls Kennzeichen und Zeitpunkt erfasst. Abhängig von diesen Daten erfolgt die weitere Verarbeitung:

   a) Das Kennzeichen wurde von der Einfahrstation nicht übermittelt:
      Das Fahrzeug hat seine Fahrt innerhalb des Messbereichs begonnen. Da eine Messung nicht möglich ist, wird der Datensatz sofort verworfen.

   b) Das Kennzeichen wurde von der Einfahrstation übermittelt und die Referenzzeit ist überschritten:
      Das Fahrzeug hat entweder seine Fahrt im Messbereich beendet oder ist langsamer als die vorgeschriebene Höchstgeschwindigkeit. Damit ist entweder keine Messung möglich oder es liegt kein Geschwindigkeitsverstoß vor – der Datensatz wird verworfen.

   c) Das Kennzeichen wurde von der Einfahrstation übermittelt und die Referenzzeit wurde unterschritten:
      Es liegt ein Geschwindigkeitsverstoß vor, die Mess- und Erfassungseinheit fertigt ein Foto des Fahrzeugführers an und legt zusammen mit den Daten der Ein- und Ausfahrstation einen signierten und verschlüsselten Datensatz an. Dieser wird zur Weiterverarbeitung entweder auf dem Gerät abgelegt (manuelle Abholung) bzw. automatisiert an eine Zentraleinheit weitergeleitet.

Rechtliche Bewertung

Mit der Section-Control sollen Geschwindigkeitsübertretungen erfasst werden, die dann im Rahmen eines Ordnungswidrigkeitsverfahrens geahndet werden. Für ein Ordnungswidrigkeitsverfahren dürfen gem. § 100h Abs. 1 Ziff. 1 StPO i. V. m. § 46 OWiG Bildaufnahmen erstellt werden. Dies hat das Bundesverfassungsgericht in einem Beschluss vom 07.05.2010 (Az. 2 BvR 759/10) ausdrücklich klargestellt.

§ 100h Abs. 1 StPO

Auch ohne Wissen der Betroffenen dürfen außerhalb von Wohnungen

1. Bildaufnahmen hergestellt werden,
2. sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,

wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgsversprechend oder erschwert wäre. Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

Allerdings darf eine solche Aufnahme nur von Beschuldigten erstellt werden. Zum Zeitpunkt des Einfahrens in den Kontrollbereich kann jedoch noch nicht festgestellt werden, ob der Fahrzeugführer im Weiteren eine Ordnungswidrigkeit begehen wird. Insoweit ist die Situation vergleichbar mit dem Einsatz der automatischen Kennzeichenerkennung auf Grundlage des Polizeirechts.

Das Bundesverfassungsgericht hat zum Einsatz der dazu notwendigen Lesegeräte festgestellt, dass eine Erfassung von Informationen dann nicht als Datenerhebung zu bewerten ist, wenn ein Abgleich von erfassten Kennzeichen mit einer Liste der gesuchten Kennzeichen unverzüglich erfolgt und die sogenannten Negativ-Treffer ohne weitere Auswertung sofort und spurenlos gelöscht werden. Somit erfolgt beim Einsatz einer entsprechenden Technik auch kein Eingriff in das Recht auf informationelle Selbstbestimmung. (Urteil vom 11.03.2008 – 1 BvR 2074/05 u. a. – BVerfGE 120, 378 ff.)

Auf Grundlage dieser Rechtsprechung habe ich das vorgestellte Projekt zur Section-Control bewertet. Es werden nur solche Datensätze weiterverarbeitet, bei denen der Abgleich der zugehörigen Zeitstempel zur Feststellung einer Geschwindigkeitsverletzung geführt hat. Alle anderen erfassten Informationen werden nach Ablauf der Referenzzeit unverzüglich gelöscht. Es ist sichergestellt, dass beim Öffnen der Säulen die im Hauptspeicher vorhandenen Daten gelöscht werden, und somit ein Zugriff auf alle Informationen, die nicht zur Feststellung einer Geschwindigkeitsverletzung geführt haben, ausgeschlossen ist. Daher kann das vorgestellte Projekt als ein entsprechend geschlossenes System betrachtet werden. Alle angefallenen Daten zu Fahrzeugen, für die beim Verlassen der Messstrecke kein Verkehrsverstoß festgestellt wird, werden unmittelbar im System gelöscht.

Dies bedeutet im Sinne der Aussagen des Bundesverfassungsgerichts, dass nur die Daten der Fahrzeuge erhoben werden, für die ein Geschwindigkeitsverstoß festgestellt ist. Deshalb habe ich die Durchführung des Pilotprojekts für zulässig eingestuft.

6. Landkreise und Kommunen

6.1
Wahl hauptamtlicher Beigeordneter

In einer hessischen Kommune wurde anlässlich der Wahlvorbereitung zur Wahl eines hauptamtlichen Beigeordneten Beschwerde bezüglich des mit der Wahlvorbereitung betrauten Haupt- und Finanzausschusses geführt. Im Einzelnen wurden angeführt, dass sich Ausschussmitglieder bei Sitzungen von Nichtausschussmitgliedern vertreten ließen und auch keine Konstituierung des Ausschusses erfolgt sei. Insbesondere die Frage der Vertretungen in Sitzungen im Zusammenhang mit der Wahlvorbereitung bedarf einer datenschutzrechtlichen Betrachtung.

Der Wahl hauptamtlicher Beigeordneter einer Kommune gehen eine entsprechende Ausschreibung und ein Bewerbungsverfahren voraus. In diesem Verfahren werden die Bewerbungsunterlagen einem bestimmten Personenkreis zugänglich gemacht. Diese Bewerbungsunterlagen beinhalten regelmäßig Informationen nicht nur über Ausbildung und den beruflichen Werdegang, sondern auch ergänzend Informationen zu persönlichen und familiären Verhältnissen, unter Umständen auch über Erkrankungen oder Behinderungen. Das Zugänglichmachen dieser Informationen muss sich daher streng an einem zugrundeliegenden Erfordernis der Kenntnisnahme orientieren, was der Gesetzgeber auch in den Regelungen des § 42 HGO festgeschrieben hat.

§ 42 Abs. 2 HGO

Die Wahl der hauptamtlichen Beigeordneten wird durch einen Ausschuss der Gemeindevertretung vorbereitet. Die Sitzungen dieses Ausschusses sind nicht öffentlich; der Vorsitzende der Gemeindevertretung und seine Stellvertreter, sofern sie nicht Ausschussmitglieder sind, sonstige Gemeindevertreter – mit Ausnahme der Minderheitenvertreter nach § 62 Abs. 4 Satz 2 – und die Beigeordneten können nicht an den Ausschusssitzungen teilnehmen; über das Ergebnis der Sitzungen dürfen nur an Mitglieder der Gemeindevertretung und des Gemeindevorstands Auskünfte erteilt werden. Die Stellen der hauptamtlichen Beigeordneten sind öffentlich auszuschreiben. Der Ausschuss hat über das Ergebnis seiner Arbeit in einer öffentlichen Sitzung der Gemeindevertretung zu berichten. Satz 1 bis 4 gelten nicht für die Fälle der Wiederwahl.

Bei der Betrachtung des Zwecks der Norm ist es daher auch unerheblich, ob zur Vorbereitung der Wahl hauptamtlicher Beigeordneter ein Wahlvorbereitungsausschuss eingesetzt wird oder ein bestehender Ausschuss – wie beispielsweise ein Haupt- und Finanz-ausschuss – mit dieser Aufgabe betraut wird. Die restriktiven Regelungen des § 42 HGO betreffen damit auch einen bestehenden Haupt- und Finanzausschuss, soweit dieser zur Wahlvorbereitung bestimmt wurde.

Aus datenschutzrechtlicher Hinsicht sind insbesondere der Ausschluss der Öffentlichkeit bei den Sitzungen und die ausschließliche Teilnahme der Ausschussmitglieder zu beachten, damit die inhaltlichen Informationen zu den Bewerberinnen und Bewerbern nur dem Personenkreis zugänglich sind, denen die Wahlvorbereitung auch obliegt. Vertretungsregelungen sind in diesem Kontext nur im Hinblick auf die Funktionsfähigkeit zum Zweck der Wahlvorbereitung tolerabel. Dies bezieht sich nicht nur auf den Personenkreis, der an einer Entscheidungsfindung beteiligt ist, sondern auch auf die Personen, die rein administrative Tätigkeiten beisteuern, wie beispielsweise Schriftführerinnen und Schriftführer. Die Ausgestaltung des Ausschusses sollte dahingehend ausgerichtet sein, auch bei einzelnen Ausfällen von Mitgliedern noch handlungsfähig zu sein und trotzdem der hier in besonderem Maße geforderten Diskretion im Hinblick auf Persönlichkeitsrechte der Bewerberinnen und Bewerber gerecht werden zu können.

Ergebnismitteilungen seitens des Ausschusses dürfen demnach auch keine individuellen Informationen zu den erfolgten Beratungen des Ausschusses beinhalten, die personenbezogenen sind oder mittelbar eine Personenbeziehbarkeit entwickeln, soweit dies nicht unvermeidbar ist.

6.2
Weitergabe von Ergebnisniederschriften

Die Ergebnisprotokolle der Gemeinderatsitzungen dürfen nur an die Vorsitzenden der Gemeindevertretung und an Fraktionsvorsitzende übersendet werden.

Der Anlass

Eine Kommune fragte bezüglich der Zulässigkeit der Weitergabe der gekürzten Magistratsprotokolle bzw. Protokolle des Gemeindevorstands an Fraktionsmitglieder der Stadtverordnetenversammlung bzw. Gemeindevertretung nach. Es bestand der Verdacht, dass ein Fraktionsvorsitzender regelmäßig die Protokolle an seine Fraktionsmitglieder weitergab.

Rechtliche Bewertung

Eine einschlägige Regelung hierzu findet sich in § 50 Abs. 2 Satz 4 HGO.

§ 50 Abs. 2 Satz 4 HGO

Die Überwachung erfolgt unbeschadet von Satz 2 durch Ausübung des Fragerechts zu den Tagesordnungspunkten in den Sitzungen der Gemeindevertretung, durch schriftliche Anfragen und auf Grund eines Beschlusses der Gemeindevertretung durch Übersendung von Ergebnisniederschriften der Sitzungen des Gemeindevorstands an den Vorsitzenden der Gemeindevertretung und die Vorsitzenden der Fraktionen.

Hier ist die Weitergabe der gekürzten Magistratsprotokolle, im Gesetz als Ergebnisniederschrift bezeichnet, abschließend geregelt. Demnach dürfen beim Vorliegen eines korrespondierenden Beschlusses der Gemeindevertretung die Ergebnisniederschriften der Sitzungen des Gemeindevorstandes an den Vorsitzenden der Gemeindevertretung und die Fraktionsvorsitzenden übersandt werden, nicht aber an die Mitglieder der Fraktionen.

Diese Regelung dient auch in datenschutzrechtlicher Hinsicht dem Erfordernis einer vertraulichen Behandlung von Ergebnissen aus Sitzungen des Gemeindevorstandes bzw. des Magistrats, die sich explizit auf die reinen Ergebnisprotokolle bezieht. Nach einem gesetzeskonformen Versand an den bezeichneten Personenkreis obliegt die weitere Wahrung der Vertraulichkeit den Adressaten im Rahmen der Vorschriften zur Verschwiegenheitspflicht der Mandatsträger gemäß § 24 HGO. Danach ist eine Weiterleitung durch die Fraktionsvorsitzenden rechtlich unzulässig. Soweit die Ergebnisniederschriften seitens der zur Verschwiegenheit verpflichteten Adressaten einem erweiterten Personenkreis zugänglich gemacht werden, könnte sogar ein ordnungswidriger Tatbestand nach § 24a Abs. 1 Nr. 2 i. V. m. § 24 HGO erfüllt sein. Die für die Verfolgung einer solchen Ordnungswidrigkeit zuständige Verwaltungsbehörde ist

gemäß § 24a Abs. 3 HGO der Gemeindevorstand, der im Rahmen des Opportunitätsprinzips hier eine Entscheidung treffen muss.

6.3
Inhalt einer Wahlhelferdatei

In den Wahlhelferdateien der Kommunen und Kreise dürfen nur die Daten verarbeitet werden, die in den Wahlgesetzen katalogmäßig aufgeführt sind. Dazu gehört nicht eine Parteizugehörigkeit.

In diesem Jahr habe ich, auch vor dem Hintergrund der Bundestagswahlen, in drei Kommunen die Vorgehensweisen im Zusammenhang mit der Erfassung und Pflege des Datenbestandes in den sogenannten Wahlhelferdateien geprüft.

Sowohl § 9 Abs. 4 BWG als auch § 15 Abs. 4 LWG und § 6 Abs. 4 KWG sehen vor, dass Mitglieder von Wahlvorständen in einer Datei gespeichert werden dürfen.

In den genannten Vorschriften befindet sich jeweils ein übereinstimmender Katalog der Daten, die in diesem Zusammenhang erhoben und verarbeitet werden dürfen. Hierbei handelt es sich um Name, Vorname, Geburtsdatum, Anschrift, Telefonnummern, Zahl der Berufungen zu einem Mitglied der Wahlvorstände und die dabei ausgeübte Funktion. Alleine im Bundeswahlgesetz befindet sich ergänzend noch, dass auch die Art der Wahl, für die der Betroffene eingesetzt wurde, erfasst werden darf.

In den drei von mir geprüften Kommunen war die jeweilige Wahlhelferdatei in das zu Wahlen eingesetzte Computerprogramm „PC Wahl“ integriert, welches hierfür eine entsprechende Datenverarbeitungsebene anbietet. Neben den oben genannten, gesetzlich abschließend aufgeführten Daten bietet das Programm ergänzend die Möglichkeit, ein Datenfeld „Beruf“ sowie ein Datenfeld „Parteizugehörigkeit“ zu befüllen. Meine Prüfung ergab, dass tatsächlich in keinem Fall das Datenfeld „Beruf“ befüllt worden war, jedoch in einigen Fällen eine Parteizugehörigkeit einer Person im Datensatz abgebildet war. Das Erheben und Verarbeiten dieser Daten ist rechtlich nicht gedeckt und damit unzulässig.

Auch das Gebot des § 5 Abs. 3 Satz 2 KWG, bei der Berufung der Beisitzer die im Wahlkreis vertretenen Parteien und Wählergruppen nach Möglichkeit zu berücksichtigen, kann keine

Rechtsgrundlage für das Erheben und Verarbeiten weiterer personenbezogener Daten zur Wahlhelferdatei darstellen.
Nach Rücksprache mit dem Hessischen Innenministerium besteht Einvernehmen darüber, dass ausschließlich die in den Wahlgesetzen aufgelisteten Daten erhoben und verarbeitet werden dürfen. In einem entsprechenden Erlass vom 11.09.2017 wurden die Kreisausschüsse der Landkreise und die Magistrate der kreisfreien Städte hierauf hingewiesen.

6.4
Datenverarbeitung bei den Bezirksschornsteinfegern

Die nach § 8 des Gesetzes über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk (SchfHwG) bevollmächtigten Schornsteinfeger nehmen hoheitliche Aufgaben wahr und dürfen die personenbezogenen Daten, die ihnen bei Kontrollen von Feuerstätten bekannt geworden sind, nur zu den im SchfHwG genannten Zwecken verarbeiten. Eine Verwendung dieser Daten zu eigenen gewerblichen Zwecken ist unzulässig.

Verschiedentlich wurde ich im Berichtsjahr gefragt, ob die nach § 8 SchfHwG bevollmächtigten Schornsteinfeger die Daten aus den Feuerstätten-Kontrollen auch zu gewerblichen Zwecken verwenden dürfen. Des Weiteren bestand Unsicherheit, was bei einer Kehrbezirksübergabe hinsichtlich der angefallenen personenbezogenen Daten zu beachten und wie in einem Vertretungsfall mit den Daten umzugehen ist.

Welche personenbezogenen Daten die bevollmächtigten Schornsteinfeger zu welchen Zwecken verarbeiten dürfen, ergibt sich aus dem Schornsteinfegerhandwerkgesetz und hier insbesondere aus der Vorschrift über das Führen des Kehrbuchs; denn als Grundlage für die Kontrolle der Kehr- und Überprüfungspflichten sowie der Pflichten nach der 1. Bundesimmissionsschutzverordnung (BImSchV) führen die bevollmächtigten Bezirksschornsteinfeger das sog. Kehrbuch. Dort sind neben den Eigentümer- und Besitzerdaten die Stammdaten jeder Feuerungsanlage einzutragen sowie das Datum der vorgeschriebenen Arbeiten, eventuelle Mängel an der Anlage sowie das Datum, an dem der Mangel abgestellt wurde. Welche Daten im Einzelnen einzutragen sind, ergibt sich aus § 19 Abs. 1 SchfHwG.

§ 19 Abs. 1 SchfHwG

In das Kehrbuch sind die folgenden Daten einzutragen:
1. Vor- und Familienname sowie Anschrift

a) des Eigentümers, und falls davon abweichend, des Besitzers oder
b) des Verwalters nach § 20 des Wohnungseigentumsgesetzes im Fall von Wohnungseigentum und, wenn die Anlage zum Sondereigentum gehört, des Wohnungseigentümers und, wenn davon abweichend, des Besitzers, oder
c) der Wohnungseigentümer, wenn kein Verwalter bestellt ist, und, wenn abweichend, der Besitzer;

2. Art, Brennstoff, Nennwärmeleistung und Alter der Anlage sowie Angaben über ihren Betrieb, Standort und ihre Zuweisung zur Abgasanlage;
3. die nach den Rechtsverordnungen nach § 1 Abs. 1 Satz 2 und 3 und die nach der Verordnung über kleine und mittlere Feuerungsanlagen vorgeschriebenen und nach § 14a festgesetzten Arbeiten und das Datum der Ausführung;
4. das Datum und das Ergebnis der letzten beiden Feuerstättenschauen;
5. in dem Formblatt nach § 4 vermerkte Mängel oder selbst festgestellte Mängel und das Datum des Abstellens der Mängel;
6. das Datum und das Ergebnis einer Bauabnahme nach Landesrecht;
7. der Anlass, das Datum und das Ergebnis einer Überprüfung nach § 15 Satz 1;
8. die für die Aufstellung von Emissionskatastern im Sinne des § 46 des Bundesimmissionsschutzgesetzes erforderlichen Angaben nach Maßgabe der öffentlich-rechtlichen Vorschriften auf dem Gebiet des Immissionsschutzes.

Soweit die in Satz 1 genannten Daten den bevollmächtigten Bezirksschornsteinfegern nicht ohnehin auf Grund ihrer Tätigkeiten bekannt sind, entnehmen sie die Daten den ausgefüllten Formblättern nach § 4.

Diese Daten darf der bevollmächtigte Schornsteinfeger nur zur Erfüllung seiner hoheitlichen Aufgaben aus dem SchfHwG verwenden und nicht für eigene gewerbliche Zwecke. Allerdings dürfen die personenbezogenen Daten aus dem Kehrbuch dann an Dritte übermittelt werden, wenn dies nach Landesrecht zulässig ist, der Dritte ein rechtliches Interesse an der Kenntnis der Daten hat und der von der Datenübermittlung Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat (§ 19 Abs. 5 Satz 3 Nr. 2 SchfHwG).

Im Falle einer Übergabe des Bezirks an einen nachfolgenden Schornsteinfeger hat der bisherige Schornsteinfeger das Kehrbuch und die für die Führung des Kehrbuchs erforderlichen Unterlagen und gespeicherten Daten kostenfrei und vollständig zu übergeben. Gleichzeitig hat der zur Übergabe Verpflichtete alle durch die hoheitliche Tätigkeit erlangten Daten bei sich zu löschen (§ 19 Abs. 3 SchfHwG).

Ist der bevollmächtigte Schornsteinfeger an der Ausübung seiner Tätigkeit verhindert, so kann ein benachbarter Bezirksschornsteinfeger mit der Aufgabe betraut werden. Dazu sind diesem die dafür erforderlichen Daten und Unterlagen vorab zur Verfügung zu stellen (§ 11 Abs. 3 SchfHwG). Nach dem Ende der Vertretung sind die Daten wieder dem zuständigen Bezirksschornsteinfeger zurückzugeben.

6.5
Weiterleitung von Patientendaten für Kurkarten

Die Übermittlung von Patientendaten von Reha- und Kurkliniken an eine Kur- und Kongreß-GmbH zum Zwecke der Ausstellung von Kurkarten bedarf regelmäßig einer Satzung nach dem Kommunalen Abgabengesetz.

Der Anlass

Im vergangenen Jahr wandte sich der Gast einer Kurklinik in Bad Homburg v. d. Höhe an mich. Dieser war überrascht, dass im Rahmen der Erhebung des Kurbeitrages auch personenbezogene Daten von ihm an eine Kur- und Kongreß-GmbH weitergeleitet wurden. Die Bedenken bezogen sich darauf, dass bereits aus der Spezialisierung der Klinik ersichtlich sei, woran der Patient wahrscheinlich erkrankt sei, und in das Verfahren der Kurkartenvergabe eine weitere Stelle außerhalb des Krankenhauses eingeschaltet wurde.

Als Begründung wurde dem Beschwerdeführer von Seiten des Krankenhauses der § 6 der Satzung über die Erhebung eines Kurbeitrages in Bad Homburg v. d. Höhe genannt. Danach seien Kurklinken dazu verpflichtet, bei ihnen aufgenommene Personen durch Vorlage des Verzeichnisses gemäß § 28 Abs. 2 Hessisches Meldegesetz (HMG) anzumelden (§ 6 Abs. 1 Satz 4 der Satzung). Wie § 6 Abs. 2 darüber hinaus regele, sollen Meldungen nach § 6 Abs. 1 an die Kur- und Kongress-GmbH gerichtet werden.

Der Beschwerdeführer entgegnete, dass Personen, die in Krankenhäusern, Sanatorien, Heil- und Pflegeanstalten aufgenommen werden, gemäß § 28 Abs. 2 HMG nicht der allgemeinen Meldepflicht unterliegen. Danach seien die genannten Einrichtungen nur dazu verpflichtet, die Identitäten der aufgenommenen Personen in einem Verzeichnis zu vermerken. Meldungen daraus seien lediglich an Polizeibehörden, Staatsanwaltschaften sowie die zuständigen Meldebehörden zu machen, wenn dies zur Abwehr erheblicher Gefahren, zur Verfolgung von

Straftaten, oder zur Aufklärung des Schicksals von Vermissten und Unfallopfern im Einzelfall erforderlich sei. Zudem sei zu beachten, dass das Hessische Meldegesetz inzwischen außer Kraft getreten ist. Seit dem 01.11.2015 gelte das Bundesmeldegesetz (BMG). Auch dieses Gesetz sehe keine entsprechende Regelung für die Übermittlung von Meldedaten vor, sofern es sich um Kur- oder Rehakliniken handele.

Rechtliche Bewertung

In meine Bewertung war mit einzubeziehen, ob die Daten, die Gegenstand der Übermittlung waren, tatsächlich in ihrer Gesamtheit erforderlich sind. Hierzu gehörten neben dem Gastnamen, der Anschrift, dem An- und Abreisedatum, der Versicherungsart und der Staatsangehörigkeit auch das Geburtsjahr und die Passnummer.

Im Ergebnis hatte der Beschwerdeführer Recht. Das Melderecht sieht keine Regelung vor, die die Datenübermittlung zulässt. Jedoch bietet § 13 Abs. 3 des Gesetzes über kommunale Abgaben (KAG) eine geeignete Rechtsgrundlage für das Vorgehen.

§ 13 Abs. 3 KAG

Wer Personen gegen Entgelt beherbergt, kann durch die Satzung verpflichtet werden, die beherbergten Personen der Gemeinde zu melden. Er kann ferner verpflichtet werden, den Kur- oder Tourismusbeitrag einzuziehen und an die Gemeinde abzuliefern; er haftet insoweit für die rechtzeitige Einziehung und vollständige Ablieferung des Kur- und Tourismusbeitrages. Dies gilt auch für die Inhaber von Sanatorien, Kuranstalten und anderen Einrichtungen, die Kur-, Erholungs-, oder sonstigen Fremdenverkehrszwecken dienen.

Der Dialog mit dem Magistrat der Stadt Bad Homburg v. d. Höhe gestaltete sich zunächst schwierig. Auch eine zwischenzeitlich praktizierte Übergangslösung, bei der Patientennummern aus dem Krankenhausinformationssystem (KIS) heraus zur Identifizierung der Patienten verwendet werden, entsprach nicht meinen Vorgaben. Insbesondere handelte es sich um kein Verfahren, bei dem mit anonymisierten Daten gearbeitet wird, so dass von dem Erfordernis einer Rechtsgrundlage oder einer Einwilligung abgesehen werden konnte.

Etwa ein Jahr nach der Eingabe teilte mir der Magistrat der Stadt Bad Homburg v. d. Höhe mit, dass er eine Änderungssatzung zur Satzung über die Erhebung eines Kurbeitrages in Bad

Homburg v. d. Höhe vom 22.06.1987 erstellen wird. Der entsprechende Entwurf wurde in der Folge mit mir abgestimmt. Er stützt sich auf § 13 Abs. 3 S. 3 KAG.

Zu den personenbezogenen Daten der Patienten, die an die Kur- und Kongreß-GmbH zum Zwecke der Kurkartenerstellung sowie der Kurkartenabrechnung übermittelt werden, zählen nunmehr nur noch die erforderlichen Daten, nämlich der Name des Patienten, das An- und Abreisedatum, der Wohnort sowie die Information, ob es sich um einen Vollzahler oder eine Begleitperson handelt. Die genannte Änderungssatzung wurde am 02.11.2017 von der Stadtverordnetenversammlung beschlossen.

Ausblick

Zum jetzigen Zeitpunkt gehe ich davon aus, dass noch in weiteren Gemeinden im Hinblick auf das geschilderte Verfahren ein Anpassungsbedarf besteht. Die jeweils zuständigen Datenschutzbeauftragten sollten daher noch einmal selber prüfen, ob die jeweiligen Rechtsgrundlagen noch aktuell sind oder einer Anpassung bedürfen. Gleichermaßen ist ein Augenmerk darauf zu richten, ob die im Kontext der Kurkartenausgabe erhobenen Daten tatsächlich in dem entsprechenden Umfang erforderlich sind.

7. Gesundheit und Forschung

7.1
Unberechtigte Zugriffe auf ein Krankenhausinformationssystem (KIS)

Ein erneuter Fall unberechtigter interner Zugriffe auf Patientenakten zeigt, dass neben der technischen Umsetzung eines angemessenen Rollen- und Berechtigungskonzepts für die Zugriffe auf das Krankenhausinformationssystem auch organisatorische Maßnahmen erforderlich sind, um ein angemessenes Datenschutzniveau im Krankenhaus zu gewährleisten.

Der Anlass

In meinen Tätigkeitsberichten habe ich mich immer wieder ausführlich mit dem Thema Rollen- und Berechtigungskonzepte für die Zugriffe auf Krankenhausinformationssysteme befasst. Patienten gehen nicht davon aus und müssen nicht davon ausgehen, dass die gesamte Belegschaft eines Krankenhauses ihre Krankheitsdaten zur Kenntnis nehmen kann. Das entsprechende Rollen- und Berechtigungskonzept und dessen Umsetzung haben sicher zu stellen, dass Mitarbeiter im Klinikum nur Zugriff auf die Patientendaten haben, die sie tatsächlich für ihre Aufgabenerfüllung benötigen.

Bereits im letzten Jahr habe ich über einen Vorfall im Klinikum Höchst berichtet, bei dem es zu unberechtigten Zugriffen auf Patientenakten von Mitarbeitern durch andere Mitarbeiter kam. Die Geschäftsleitung der Klinik hatte daraufhin zugesichert, ab dem 1. Quartal 2017 stichprobenhafte Kontrollen der Zugriffe auf Krankenakten einschließlich einer Dokumentation der erfolgten Kontrollen und veranlassten Maßnahmen einzuführen. Ebenso war es angedacht, daran zu arbeiten, Einschränkungen des Zugriffskonzepts sowie eine umfangreiche Anpassung des Rollen- und Berechtigungskonzeptes vorzunehmen.

Im Sommer wurde mir aus dem Klinikum Höchst erneut ein Vorfall gemeldet, bei dem Mitarbeiter auf Patientendaten ihrer Kollegen zugegriffen hatten.

Bei den Ermittlungen des Sachverhaltes stellte sich heraus, dass die betroffenen Mitarbeiterinnen aus dem Schreibdienst, organisatorisch bedingt, umfassende Lese- und Schreibrechte auf Patientendaten hatten und dementsprechend auch auf die Patientendaten ihrer Kollegen zugreifen konnten. Weiterhin stellte sich bei der Auswertung der entsprechenden Protokollda-

ten heraus, dass vermutlich von einer Mitarbeiterin sogar Änderungen an der eigenen Patientenakte vorgenommen wurden. Was genau geändert wurde, ließ sich jedoch nicht mehr nachvollziehen.

Ein geeignetes Konzept, wie mit Mitarbeitern, die im eigenen Krankenhaus behandelt werden, umzugehen ist, gab es nicht. Ebenso war die eingesetzte KIS-Software laut Klinik bislang nicht in der Lage, eine technische Lösung anzubieten, die Mitarbeiterdaten sinnvoll schützt.

Rechtliche Bewertung

Beschäftigte des Krankenhauses als Patienten müssen davor geschützt werden, dass Kolleginnen und Kollegen von ihrem Aufenthalt erfahren (können), die nicht unmittelbar an der Behandlung beteiligt sind.

Die Patientendaten der Mitarbeiter haben dementsprechend einen besonderen Schutzbedarf. Als Orientierungsrahmen, wie eine datenschutzkonforme Ausgestaltung und ein datenschutzgerechter Betrieb entsprechender Verfahren zu erfolgen hat, kann die von den Datenschutzbeauftragten des Bundes und der Länder erstellte Orientierungshilfe für Krankenhausinformationssysteme (OH KIS) dienen.

Danach sollen die Fallakten im KIS bei Bedarf dahingehend gekennzeichnet werden, dass der Patient Mitarbeiter des behandelnden Krankenhauses ist. Die Struktur des Rollen- und Berechtigungskonzepts soll so angepasst werden, dass an diese Kennzeichnung besondere Zugriffsregelungen geknüpft werden können (Teil I, Tz. 42).

Solange das eingesetzte KIS keine ausreichenden technischen Möglichkeiten bietet, die Patientendaten der Mitarbeiter zu schützen, müssen angemessene organisatorische Maßnahmen ergriffen werden, um die Mitarbeiterdaten zu schützen. Neben der datenschutzrechtlichen Sensibilisierung der Mitarbeiter gewinnt dabei die Protokollierung der Zugriffe im KIS und deren Auswertung besondere Bedeutung für die datenschutzgerechte Ausgestaltung des KIS. Dabei kann in Bereichen mit einem hinreichend fein differenzierten Zugriffsschutz im KIS die Protokollierung und auch die Auswertung der Protokolle reduziert werden. Umgekehrt steigt ihre Bedeutung in den Bereichen mit sehr weit gefassten Zugriffsberechtigungen.

Entsprechend den Forderungen in der OH KIS ist ein Verfahren für regelmäßige, verdachtsunabhängige Kontrollen sowie für Fälle eines Verdachts auf unberechtigten Zugriff vorzusehen, dass auch den besonderen Schutzbedarf der Patientendaten von Mitarbeitern berücksichtigt. Außerdem ist es zum Nachweis der fehlerfreien und ordnungsgemäßen Datenverarbeitung (§ 10 Abs. 2 HDSG) erforderlich, dafür Sorge zu tragen, dass es Mitarbeitern nicht möglich ist, unkontrolliert Änderungen an ihren eigenen Patientenakten vorzunehmen.

Meine Forderung an das Klinikum Höchst

Gegenüber dem Klinikum habe ich gefordert, dass das vorhandene Rollen- und Berechtigungskonzept weiter überarbeitet wird. Zudem ist an technischen Maßnahmen zu arbeiten, die die Möglichkeit eines unberechtigten Zugriffs auf Mitarbeiter-/Patientendaten noch einmal reduzieren.

Solange das eingesetzte KIS technisch nicht in der Lage ist, die Patientendaten der Mitarbeiter ausreichend zu schützen, sind zusätzliche organisatorische Maßnahmen zu ergreifen. Neben der Sensibilisierung der Mitarbeiter sind 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 (§ 10 Abs. 2 HDSG). Entsprechend den Forderungen in der OH KIS ist ein Verfahren für regelmäßige, verdachtsunabhängige Kontrollen sowie für Fälle eines Verdachts auf unberechtigte Zugriffe vorzusehen. Dabei sind Fallakten von Mitarbeitern in einem angemessenen Umfang mit einzubeziehen. Im Interesse der Transparenz für alle Beteiligten ist das entsprechende Protokollierungs- und Auswertungskonzept allen Mitarbeitern des Klinikums bekannt zu machen.

Weiterhin ist für eine datenschutzgerechte Gestaltung des KIS und einer angemessenen Nachvollziehbarkeit der Verarbeitung personenbezogener Daten eine aussagefähige und revisionsfeste Protokollierung schreibender und lesender Zugriffe notwendig. Zudem sind geeignete Auswertungsmöglichkeiten erforderlich. Dass ein Mitarbeiter seine eigene Akte bearbeiten kann und dies dann für das Krankenhaus nicht einmal im Detail nachvollziehbar ist, ist durch geeignete Maßnahmen zu verhindern.

Auch das bisherige „VIP-Konzept“ des Klinikums ist nicht ausreichend. Letztlich bestand dieses nur darin, die ausgewählten Patientinnen oder Patienten in der Pförtnerliste auszublenden.

Gerade für „VIPs“, die im Krankenhaus behandelt werden, müssen eine geeignete technische Lösung und ein organisatorisches Konzept implementiert sein, die dem erhöhten Schutzbedarf dieser Personengruppen gerecht werden. Meine Forderung ist daher, ein entsprechendes Konzept auszugestalten. Zugleich ist zu prüfen, ob dieses Konzept dann auch für Mitarbeiter Verwendung finden kann.

Da es in den vergangenen Jahren im Klinikum wiederholt zu unberechtigten Zugriffen auf Patientendaten von Mitarbeitern gekommen ist, lässt dies vermuten, dass es einzelnen Mitarbeitern an der entsprechenden Sensibilität für den Datenschutz mangelt. Es sind daher geeignete Maßnahmen zu ergreifen, um das Datenschutzbewusstsein der Mitarbeiter zu verbessern (z. B. Schulungen, Infos etc.).

Ich werde das Klinikum auf dem Weg zu einer Lösung, die diesen Forderungen gerecht wird, weiter aufsichtsrechtlich und beratend begleiten.

7.2
Einsatz von Trackingverfahren im Rahmen klinischer Prüfungen

Bei Forschungsvorhaben im Bereich der klinischen Forschung kommen zunehmend neue Technologien zum Einsatz, die eine besondere Berücksichtigung von datenschutzrechtlichen Aspekten verlangen.

Bei der im Folgenden geschilderten Studie habe ich mein Augenmerk auf das mittels einer Smartwatch geplante Aktivitätstracking sowie das damit einhergehende Geofencing gerichtet und diesbezüglich datenschutzrechtliche Vorgaben formuliert.

Der Hintergrund

Ein forschendes Unternehmen informierte mich, dass es eine klinische Prüfung zur Brustkrebstherapie plane, die als Besonderheit ein Begleitprogramm mit automatisiertem Aktivitätstracking und elektronischen Fragebögen zur Erfassung der Gesundheits- und Lebensqualität der Patienten enthält. Die Studie wurde gemäß dem Arzneimittelgesetz (AMG) bei der Ethik-Kommission der Landesärztekammer Hessen zur Bewertung eingereicht. Zur Bewertung der

datenschutzrechtlichen Aspekte fehlten der Ethik-Kommission allerdings originäre Zuständigkeit und fachliche Kenntnisse. Ich wurde daher um eine Beurteilung und Stellungnahme zu den Datenschutzaspekten des Projektes gebeten.

Bei den Patientinnen der Studie handelt es sich um Patientinnen mit Brustkrebs, der bereits begonnen hat zu streuen. Die Teilnahme an der Studie sollte grundsätzlich auf freiwilliger Basis erfolgen. Die in der Studie verabreichten Arzneimittel waren bereits zugelassen. Es war jedoch beabsichtigt, die Verträglichkeit nach der Zulassung weiter zu untersuchen.

Im Vorfeld der Behandlungsphase war es geplant, den Probandinnen eine Smartwatch auszuhändigen, die diese über sieben Tage zu tragen haben. Über diese Smartwatch wird die körperliche Aktivität der Teilnehmerinnen aufgezeichnet. Die so erhobenen Daten werden im Rahmen der Studie in Schlaf- und Aktivitätszeiten umgerechnet. Zu Beginn der Studie sollte die Probandin erneut eine entsprechende Uhr erhalten, wobei es vorgesehen ist, dass diese sechs Monate ununterbrochen Tag und Nacht zu tragen ist. Jeden Monat werden die Daten der Probandin im dafür vorgesehenen Studienzentrum ausgelesen. Die Daten gehen, nur versehen mit der ID der Uhr, an ein beauftragtes Unternehmen zur Auswertung. Ergänzend hierzu erhält die Probandin ein Smartphone, mittels dessen sie regelmäßig darauf zugesandte Fragen zu beantworten hat.

In einem freiwilligen Modus ist es geplant, über ein sogenanntes Call-Tracking aufzuzeichnen, wie oft die Probandin mit dem behandelnden Arzt telefoniert hat. Das Call-Tracking ist insoweit auf diese Nummer beschränkt. Es handelt sich hierbei um eine optionale Funktion, die alternativ auch durch den Prüfarzt dokumentiert werden kann.

Eine weitere optionale Funktion beinhaltet den Einsatz eines sogenannten Geofencing, über das die Häufigkeit und die Dauer der Arztbesuche ermittelt werden soll. Diese Funktion wird über eine App umgesetzt. In dieser sind die Koordinaten des Studienzentrums hinterlegt. Die App erhält permanent die Standortdaten des Smartphones. Sobald der Eintritt in den „umzäunten“ Bereich erfolgt, werden die Daten in der App gespeichert und dann an den vorgesehenen Server gesendet, auf dem auch die Antworten zu den Fragebögen und die Anrufe gespeichert werden. Die Trackingfunktion speichert somit nur dann die Daten, wenn sich die Probandin in unmittelbarer Nähe des Behandlungszentrums befindet.

Wir mir dabei mitgeteilt wurde, handelt es sich bei der Arzneimittelstudie insofern um Neuland, da hierbei erstmals die genannte Smartwatch sowie das genannte Smartphone eingesetzt

werden sollen, das gewisse Trackingfunktionen ausführt. Es handelt sich um eine bundesweite Studie, von der bis auf ein Bundesland (Thüringen) alle Bundesländer betroffen sind.

Rechtliche Bewertung

Im Rahmen der Studie ergaben sich für mich schwerpunktmäßig zwei Fragen. Zum einen stand im Mittelpunkt der Überlegungen, ob der Tragezeitraum der Smartwatch von sechs Monaten und die damit einhergehende dauerhafte „Überwachung" diverser Körperfunktionen der Probandin erforderlich ist und von dieser Seite so akzeptiert werden kann. Zum anderen stellte sich die Frage, ob das hier eingesetzte Geofencing tatsächlich, auch wenn es optional ist, zugelassen werden kann. Letztlich konnte es gemäß der Mitteilung des forschenden Unternehmens nicht komplett ausgeschlossen werden, dass durch die nicht ganz exakte Ortungsmöglichkeit auch Bewegungsprofile der Probandinnen aufgezeichnet werden, die nicht im Kontext der Behandlung stehen.

Soweit dies die Dauer des Tragens der Smartwatch betrifft, wurde mir mitgeteilt, dass ursprünglich ein Tragezeitraum von 15 Monaten, mit einzelnen Unterbrechungen, vorgesehen war. Im Ergebnis wurde jedoch von potentiellen Patientinnen ein kürzerer, aber dafür kontinuierlicher Tragezeitraum befürwortet. Gemäß der forschenden Stelle bietet der letztlich gewählte zeitliche Ansatz die beste Möglichkeit, die unterschiedlichen Therapieansätze untereinander zu vergleichen. Vor dem Hintergrund der Freiwilligkeit der Teilnahme an der Studie und dem grundsätzlich auch zu beachtenden Grundsatz der Forschungsfreiheit habe ich diesbezüglich keine weiteren Einwände erhoben.

Im Hinblick auf das geplante, optionale Geofencing wurde hingegen festgestellt, dass die Ortungsfunktion nicht punktgenau auf das Prüfzentrum ausgerichtet werden kann. So ist es unter Umständen auch denkbar, dass Teilnehmerinnen an der Studie geortet werden, wenn sie regelmäßig das Prüfzentrum passieren, um zu anderen Orten zu gelangen. Aus datenschutzrechtlicher Sicht habe ich daher diese Funktion als bedenklich eingestuft. Zugleich habe ich gefordert, dass, sofern an dieser Modalität festgehalten wird, die Studienteilnehmerin zwingend darüber aufzuklären ist, dass eine punktgenaue Ortung nicht möglich ist und sie unter Umständen auch im Kontext anderer Ortsbewegung im Umfeld des Prüfzentrums Bewegungsdaten hinterlässt, die nicht im Zusammenhang mit der durchzuführenden Studie stehen. Die Aussage: „Weitere Aufenthaltsorte werden nicht erfasst" ist insoweit irreführend und nicht zutreffend.

Im Ergebnis wurde mir hierzu mitgeteilt, dass über einen Passus ergänzt wird, dass im Zweifelsfall das Geofencing für bestimmte Prüfstellen deaktiviert wird, wenn diese zum Beispiel in der Innenstadt liegen oder nicht klar zwischen verschiedenen Stationen eines Krankenhauses differenziert werden kann. Ich habe diesbezüglich noch gefordert, dass im Hinblick auf den neuen Passus zum Geofencing nicht nur Prüfstellen deaktiviert werden, die im Innenstadtbereich liegen oder bei denen nicht klar zwischen verschiedenen Stationen eines Krankenhauses differenziert werden kann, sondern auch Prüfstellen, die direkt an Verkehrsstraßen liegen. Hierzu wurde mir zugesagt, dass für jede Prüfstelle einzeln und vor Ort geprüft wird, ob ein ausreichend sauberes Geofencing möglich ist. Wenn dies nicht der Fall ist, wird das Geofencing zentrumsbasiert deaktiviert. Dies kann auch noch im Laufe der Studie erfolgen, falls Unstimmigkeiten auffallen.

Nach Prüfung der weiteren Einzelheiten zu dem Projekt wurde von mir schließlich ein positives Votum gegenüber der Ethik-Kommission und dem forschenden Unternehmen ausgesprochen.

7.3
Unsachgemäße Aufbewahrung von Laborproben im Stationsbereich eines Krankenhauses

Für Laborproben im Stationsbereich von Krankenhäusern ist grundsätzlich ein Konzept zum Zugriffsschutz vorzusehen. Insbesondere dürfen keine mit Patientendaten beschrifteten Laborröhrchen oder Auftragsscheine auf offenen Sammelplätzen allgemein zugänglich abgelegt werden.

Der Anlass

Der Patient eines Krankenhauses im Raum Frankfurt dokumentierte im letzten Jahr, auf welche Weise Blut und Urinproben auf der Station eines Krankenhauses, in dem er sich zur Behandlung befand, abgelegt werden. Der Eingebende bemängelte insoweit, dass diese Proben auf der Station des Hauses auf einem einfachen Abstellbrett im allgemeinen zugänglichen Stationsvorraum abgelegt wurden. Dort waren sie offenbar zur Abholung durch das hausinterne Labor abgelegt worden. Die Proben sind dabei standardmäßig mit Aufklebern versehen, die den Namen des Patienten, das Geburtsdatum und den Tag der Entnahme enthalten.

Meine Feststellungen vor Ort

Aufgrund dieser Information habe ich mich kurzfristig zu einem Besuch bei dem betroffenen Krankenhaus angemeldet. Der Besuch sollte unter anderem auch dazu dienen, vor Ort abzuklären, ob das dokumentierte Vorgehen tatsächlich den Regelfall darstellt. Zu klären war mithin zugleich, ob die Proben für das beauftragte Labor tatsächlich auf allen Stationen offen zugänglich abgelegt werden, um dort vom Kurierdienst abgeholt zu werden.

Wie mir bei meinem Ortstermin von der Datenschutzbeauftragten des Krankenhauses mitgeteilt wurde, habe man auf den Vorfall bereits reagiert, indem man die auf den Stationen an entsprechender Stelle angebrachten Abstellbrettchen abmontiert hat. Zudem habe es die Anweisung für die Mitarbeiter im Haus gegeben, die Proben nur im Stationszimmer abzustellen, wobei diese Anweisung offenbar lediglich mündlich erfolgt ist.

Bei meinem Besuch musste ich feststellen, dass die getroffenen Maßnahmen nicht ausreichend waren, um eine hinreichende Gewährleistung der Vorgaben des § 10 Abs. 2 Satz 2 Nr. 4 Hessisches Datenschutzgesetz (HDSG) sicher zu stellen. Darin heißt es:

§ 10 Abs. 2 HDSG

Werden personenbezogene Daten automatisiert verarbeitet, ist das Verfahren auszuwählen oder zu entwickeln, welches geeignet ist, so wenig personenbezogene Daten zu verarbeiten, wie zur Erreichung des angestrebten Zwecks erforderlich ist. Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass

...

4. personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),

Außerdem sind Maßnahmen schriftlich anzuordnen, die nach dem jeweiligen Stand der Technik und der Art des eingesetzten Verfahrens erforderlich sind, um zu gewährleisten, dass personenbezogene Daten nicht unbefugt oder nicht zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, gelöscht, entfernt, vernichtet, oder sonst verarbeitet werden (Datenverarbeitungskontrolle).

So konnte ich am frühen Morgen beobachten, dass auf einer anderen Station des Hauses gesammelte Blutproben in Kaffeebechern in dem Bereich abgestellt wurden, an dem sich vorher offenbar ein Abstellbrett befand (s. Lichtbilder).

Zu dem besagten Zeitpunkt befand sich auch keine Schwester in der unmittelbaren Nähe der Proben, so dass ohne weiteres ein Zugriff darauf hätte erfolgen können.

Bei meinem Besuch wurde mir auch gezeigt, dass auf einigen Stationen des Hauses in den Stationszimmern extra vorgesehene Fächer eingerichtet sind, in denen die Laborröhrchen für das Labor zur Abholung bereitgestellt werden. Hierbei konnte festgestellt werden, dass auch diese Fächer oftmals recht zentral am Eingangsbereich gelegen sind und insoweit auch hier unter Umständen die Datensicherheit gefährdet ist (Diebstahl der Röhrchen, Austausch der Aufkleber etc.).

Ergebnis und getroffene Maßnahmen

Als Ergebnis stand fest, dass das derzeitige Verfahren umzustellen ist. Beispielsweise könnte für die Proben ein gesicherter verschließbarer Behälter eingerichtet werden, zu dem nur die berechtigten Personen einen Zugriff haben. Eine entsprechende Sicherung kann etwa durch ein Zahlenschloss oder durch einen anderen Mechanismus erfolgen.

Wie mir das Krankenhaus im Anschluss mitteilte, wurde durch meinen Besuch deutlich, dass im Hinblick auf die Ablage der Laborproben weitere Maßnahmen zur Optimierung ergriffen werden müssen, die in den Klinikalltag zu integrieren sind. Das Krankenhaus hat sich daher

dazu entschlossen, die Laborproben auf allen Stationen des Krankenhauses direkt im Stützpunkt des Pflegepersonals abzulegen. Von dort aus werden diese dann vom internen Hol- und Bringdienst regelmäßig abgeholt. Die Türen des Stützpunktes auf den Stationen werden generell verschlossen gehalten. Ein Knauf wird zur weiteren Sicherung von außen angebracht, so dass die Öffnung nur noch mit Berechtigung erfolgen kann. Ebenso wird ein Schild vor Ort aufgehängt, welches das Eintreten nur nach Aufforderung regelt. Darüber hinaus wird ein Regalschrank im hinteren Bereich der Stationszimmer für die Ablagen der Blutproben frei geräumt, in welchem dann das gesamte organische Material bis zur Abholung aufbewahrt werden kann. Dieser Schrank ist ebenfalls mit einer Tür versehen.

Die Abholung durch den internen Hol- und Bringdienst wird durch feste Time Slots für die Zukunft geregelt, so dass jegliches organische Material innerhalb eines festen Zeitraumes abgeholt werden kann, um dieses in das hauseigene Labor zu bringen. Der Hol- und Bringdienst ist mit einem entsprechenden Chip ausgestattet, um den verschlossenen Stationsbereich ständig betreten zu können.

Eine Arbeitsanweisung, welche in das Qualitätsmanagement eingepflegt wird, wurde ebenfalls ausgearbeitet. Diese geht sowohl an den ärztlichen Dienst wie auch an das Pflegepersonal im Haus.

Die somit getroffenen Maßnahmen sind aus meiner Sicht ausreichend. Ich habe jedoch darüber hinaus aufgegeben, dass die Datenschutzbeauftragte des Krankenhauses bis Ende des Jahres unangemeldet prüft, ob die nunmehr getroffenen Regelungen auch tatsächlich dazu geeignet sind, um eine datenschutzkonforme Lagerung der Laborproben sicher zu stellen. Der entsprechende Bericht über das Ergebnis ist bis Ende des Jahres an mein Haus zu übersenden. Zugleich habe ich mir meinerseits vorbehalten, mich ebenfalls auch noch einmal bei einem unangemeldeten Kontrollbesuch von der Effektivität der ergriffenen Maßnahmen zu überzeugen.

7.4
Information über die gesetzlichen Änderungen im Bereich der ärztlichen Schweigepflicht

War ein Offenbaren der dem Berufsgeheimnisträger anvertrauten Geheimnisse und Daten bislang ohne Schweigepflichtsentbindung nur gegenüber „berufsmäßig tätigen Gehilfen“ straflos

möglich, ist mit der Neufassung von § 203 StGB eine Weitergabe des Geheimnisses an externe Personen erlaubt, die an der beruflichen oder dienstlichen Tätigkeit der Berufsgeheimnisträger mitwirken.

Outsourcing im Gesundheitsbereich

Fast jedes Unternehmen lagert heute bestimmte Bereiche des Betriebes, die man im eigenen Unternehmen nicht mehr durchführen kann oder will, an Dienstleister aus. So erfordern beispielsweise die Einrichtung, der Betrieb, die Wartung und die Anpassung der informationstechnischen Anlagen, Anwendungen und Systeme spezielle berufliche Kenntnisse, die weder beim Arzt noch bei deren Berufsgehilfen vorausgesetzt werden können. Die Einstellung von darauf spezialisiertem Personal ist jedoch vielfach wirtschaftlich nicht sinnvoll.

Eine Heranziehung Dritter zu diesen Hilfstätigkeiten war bisher für Berufsgeheimnisträger aber nicht ohne rechtliches Risiko, sofern diese Personen damit von geschützten Geheimnissen Kenntnis erlangen konnten und keine entsprechende Rechtsgrundlage oder eine Entbindung von der Schweigepflicht durch den Patienten vorhanden war.

Bisherige Rechtlage

Datenschutzrechtlich betrachtet wird bei der Beauftragung von (externen) Dienstleistern zwischen der Funktionsübertragung und der Auftragsdatenverarbeitung (ADV) unterschieden.

Bei der Funktionsübertragung werden an einen Dritten Daten übermittelt, damit dieser eine bestimmte Aufgabe eigenverantwortlich übernehmen kann. Da es sich hier um eine Datenübermittlung handelt, bedarf es einer gesetzlichen Erlaubnis oder der Einwilligung des Patienten.

Eine weitere Möglichkeit, externe Dritte einzuschalten, beinhaltet der Abschluss eines Vertrages zur Auftragsdatenverarbeitung (§ 11 BDSG, § 80 SGB X, § 4 HDSG). Bei der Auftragsdatenverarbeitung findet juristisch gesehen keine Übermittlung von Daten gegenüber Dritten statt. Daher ist in diesen Fällen aus datenschutzrechtlicher Sicht eigentlich keine spezielle Rechtsgrundlage oder die Einwilligung des Patienten erforderlich. Berufsgeheimnisträger mussten jedoch beachten, dass neben dem Datenschutzrecht auch die besonderen Geheimhaltungsinteressen gemäß § 203 StGB gewahrt bleiben.

Danach macht sich strafbar, wer ohne Einwilligung oder einer rechtlichen Grundlage ein fremdes Geheimnis offenbart, das ihm als Geheimnisträger, beispielsweise als Arzt, Apotheker, Psychologe, Rechtsanwalt, Patentanwalt, als Ehe-, Familien- oder Jugendberater oder als im öffentlichen Dienst zur Geheimhaltung verpflichteter Personen anvertraut wurde. Nach der bisher herrschenden Meinung stellte die Auftragsdatenverarbeitung nach § 11 BDSG bzw. § 4 HDSG keine ausreichende Befugnis zur Offenbarung von Patientendaten gegenüber dem Dienstleister dar. Sofern sich ein Berufsgeheimnisträger mithin eines externen Dienstleisters bedienen wollte, war bei der Auftragsdatenverarbeitung im Grunde die Entbindung von der ärztlichen Schweigepflicht durch den Patienten erforderlich, sofern sich dabei die Kenntnisnahme von Patientendaten nicht vermeiden ließ.

Da die Einschaltung von externen Dienstleistern für Berufsgeheimnisträger aber mittlerweile oft ohne Alternative, die Einholung von Schweigepflichtsentbindungen aller Patienten jedoch nicht immer umsetzbar war, setzen sich die Berufsgeheimnisträger regelmäßig der Gefahr eines Verstoßes gegen die Schweigepflicht aus, wenn sie externe Dienstleister einschalteten. Auf diese Problematik wurde von den Datenschutzaufsichtsbehörden bereits auf der 89. Konferenz der Datenschutzaufsichtsbehörden hingewiesen:

Entschließung der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 18./19.03.2015, Punkt 3

Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Neuregelung des § 203 StGB

Die Neufassung des § 203 StGB lautet nunmehr an den entscheidenden Stellen wie folgt:

§ 203 StGB

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

Mit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen hat der Gesetzgeber kurz vor Ende der

letzten Legislaturperiode den § 203 StGB angepasst, um zukünftig rechtskonforme Auftragsdatenverarbeitungen auch für Berufsgeheimnisträger zu ermöglichen.

War bisher eine Informationsweitergabe nur straffrei an „berufsmäßig tätige Gehilfen und Personen, die bei dem Berufsgeheimnisträger zur Vorbereitung auf den Beruf tätig sind“, möglich, wurde durch die Neuregelung des § 203 StGB das Offenbaren von geschützten Geheimnissen auf externe Personen erweitert, die bei der beruflichen oder dienstlichen Tätigkeit des Berufsgeheimnisträgers mitwirken.

Der neu eingeführte Begriff der mitwirkenden Person unterscheidet sich von dem des berufsmäßig tätigen Gehilfen dadurch, dass die mitwirkende Person zwar an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirkt, also in diese Tätigkeit in irgendeiner Weise eingebunden ist und Beiträge dazu leistet, allerdings ohne unmittelbar in die Sphäre des Berufsgeheimnisträgers eingegliedert zu sein.

In der Gesetzesbegründung sind einige Beispiele aufgeführt, bei denen es sich um solche mitwirkenden Tätigkeiten handeln könnte:

– Schreibarbeiten,
– Rechnungswesen,
– Annahme von Telefonanrufen,
– Aktenarchivierung und -vernichtung,
– Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art, beispielsweise auch von entsprechend ausgestatteten medizinischen Geräten,
– Bereitstellung von IT-Anlagen und Systemen zur externen Speicherung von Daten,
– Mitwirkung an der Erfüllung von buchführungs- und steuerrechtlichen Pflichten des Berufsgeheimnisträgers.

Die oben genannte Aufzählung ist sicher nicht abschließend. Jedoch begrenzt das neue Recht mit dem Merkmal der „Erforderlichkeit“ die straffreie Mitwirkung Dritter. In der Praxis wird jeweils im Einzelfall zu entscheiden sein, ob die Kenntnisnahme der Berufsgeheimnisse für die Inanspruchnahme der mitwirkenden Personen erforderlich ist.

Damit es durch die Erweiterung des Personenkreises der „Wissenden“ nicht zu einer Verringerung des Geheimnisschutzes kommt, werden die mitwirkenden Personen in die Strafbarkeit nach § 203 StGB mit einbezogen.

Darüber hinaus trifft den Berufsgeheimnisträger zukünftig die Pflicht, dafür Sorge zu tragen, dass die extern einbezogenen Personen ebenfalls zur Geheimhaltung verpflichtet werden. Die Verletzung dieser Pflicht ist strafbewehrt, wenn die einbezogene Person unbefugt ein Geheimnis offenbart hat. Die Vorschrift findet auch auf mitwirkende Personen Anwendung, die sich weiterer Personen bedienen (Unterauftragnehmer).

Fazit

Mit dem neu eingeführten § 203 Abs. 3 StGB wird ein Erlaubnistatbestand geschaffen, der die Weitergabe von Berufsgeheimnissen an Dritte für straffrei erklärt, wenn diese an der beruflichen oder dienstlichen Tätigkeit des Geheimnisträgers mitwirken. Damit können im Rahmen von Verträgen zur Auftragsdatenverarbeitung auch ohne Schweigepflichtsentbindung Patientendaten zur Kenntnis genommen werden, sofern dies erforderlich ist.

Der notwendige Schutz beruflich anvertrauter Geheimnisse wird dadurch gewährleistet, dass in einem neuen § 203 Abs. 4 StGB die Tatbestände zusammengefasst werden, nach denen sich die mitwirkende Person selbst wegen Verletzung des Privatgeheimnisses strafbar machen kann. Darüber hinaus kann der Berufsgeheimnisträger sich seinerseits strafbar machen, wenn er die mitwirkenden Personen nicht zur Geheimhaltung verpflichtet hat.

Auch wenn es sich bei der Neuregelung im Wortlaut nicht um die von meinem Haus favorisierte Version handelt, schafft der neue Gesetzestext praxisnahe Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger.

7.5
Prüfung eines Anbieters für Online-Terminbuchungen

Zu meinen Prüfungstätigkeiten im Berichtszeitraum gehörte auch die Prüfung eines Anbieters für Online-Terminbuchungen. Der Schwerpunkt lag hierbei auf dem Bereich der Arztpraxen. Sofern eine Arztpraxis entsprechende Angebote nutzt, muss auf der Homepage klar erkennbar sein, dass der Patient ein externes Angebot nutzt und nicht das der Arztpraxis. Zugleich müssen sich die E-Mails, welche die Arztpraxis zwecks der Terminbestätigung erhält, auf die tatsächlich erforderlichen Informationen beschränken.

Hintergrund

Zur Wahrnehmung meines Kontrollauftrages bin ich befugt, auch anlasslose Prüfungen von einzelnen Unternehmen vorzunehmen. Eine Prüfung bei der in Wiesbaden ansässigen Firma Terminland sollte insoweit einen Einblick in die technischen Abläufe sowie die rechtlichen Rahmenbedingungen eines externen (Internet-)Dienstleisters in Bezug auf die Terminvergabe für Arztpraxen geben.

Das von mir geprüfte Unternehmen wurde im Jahr 2003 im Kontext des neuen Geschäftsfeldes „Terminvergabe über das Internet“ gegründet. Insgesamt verwaltet Terminland etwa 6.000 Terminpläne zu einer Vielzahl von Geschäftsbereichen. Etwa 40 % der Kunden kommen aus dem medizinischen Bereich. Insgesamt gibt es im Geschäftsfeld „Terminvergabe über das Internet“ etwa 100 Anbieter in Deutschland (unter anderem Arzttermine.de, docster u. a.).

a) Terminbuchung

Am Beginn der Geschäftsbeziehung steht in der Regel ein zeitlich limitiertes Testsystem (30 Tage), das dann mit Vertragsabschluss in ein ordentliches Produktivsystem überführt wird. Der Kunde kann das System selbst einrichten, wird aber auf Wunsch auch vom Terminlandsupport unterstützt.

Die Konfiguration besteht neben den allgemeinen erforderlichen Angaben primär aus den Rahmenbedingungen für die Terminvergabe, die dann auch den Ablauf festlegen:

– Zugang zum Terminkalender (ohne Anmeldung, mit Benutzername/ Kennwort)
– Planbare Zeiträume (Geschäftsstunden)
– Fragen (erforderliche Angaben, sowohl allgemein als auch für spezielle Termine; z. B. Kasse/Privat/Selbstzahler; spezielle oder allgemeine Untersuchungen)
– Daraus resultierende Terminvergaberegeln (z. B. Privatsprechstunde nur mittwochs am Nachmittag)
– Anzeige der freien Termine
– Auswahl durch den Kunden/Patienten
– Angabe der erforderlichen Kunden-/Patientendaten (Pflicht- und freiwillige Felder)
– Zusammenfassung und Bestätigung
– Optionale Bestätigung durch den Kunden/Patienten auf einem zweiten Kanal: Bestätigungslink per E-Mail, SMS-TAN
– Wahlweise direkte, feste Eintragung des Termins oder der Buchung unter Vorbehalt (Bestätigung)

– Optional: Stornierung- und Verlegungsregelungen (z. B. Verlegung bis max. eine Stunde vor Terminbeginn)
– Löschregeln für vergangene Termine

Diese Regelungen liegen ausschließlich im Ermessen des Kunden. Dieser ist insofern z. B. allein für die Einhaltung von Aufbewahrungsfristen verantwortlich.

b) Anbindung an das Kundensystem

Der Kunde hat die Möglichkeit, seine Terminverwaltung ausschließlich im Terminland-Kalender zu führen, und die Daten aus dem Terminlandkalender manuell in sein eigenes System zu übertragen (Export/Import). Alternativ können, sofern verfügbar und von Terminland angeboten, die Daten über eine Standard-Schnittstelle mit dem System des Kunden synchronisiert werden.

c) Zugriff auf die Kundendaten

Die Verwaltung der Kundendaten erfolgt über eine eigens entwickelte Software mit einem Rollen- und Rechtekonzept. Wie mir versichert wurde, haben die Mitarbeiter von Terminland zwar Zugriff auf die Terminpläne der Kunden, sehen dort aber grundsätzlich keine Details (das heißt, sichtbar sind nur belegte und freie Terminzeiträume).

Der Zugriff auf einzelne Details des Terminplans ist nur nach Ausfüllen einer Supportmaske möglich. Dies ist im Supportsystem der Firma zwingend zu dokumentieren.

Sofern ein Zugriff auf die Daten der Kunden erforderlich ist, muss diese Freischaltung vom Kunden explizit erfolgen.

d) Protokollierung

Zum Nachvollziehen von Fehlern und Problemen erfolgt auf den Servern eine Protokollierung der Terminvergaben. Zugriff auf die Protokolle haben die Kunden, Terminland hingegen nur nach Freigabe durch den Kunden.

Wie mir zudem versichert wurde, findet eine Analyse der Kundendaten durch Terminland nicht statt. Auf der Webseite ist lediglich ein Zähler aller über das System vergebenen Termin eingebaut, der periodisch aktualisiert wird (kein Echtzeit-Zähler).

Datenschutzrechtliche Bewertung und eingeforderte Maßnahmen

a) Überarbeitung von Kunden- und Patienteninformationen

Wie mir bei meinem Besuch entsprechend den oben genannten Ausführungen mitgeteilt wurde, haben die Mitarbeiter von Terminland zwar grundsätzlich einen Zugriff auf die Terminpläne der Kunden, sie sehen dort aber keine Details. Sofern im Einzelfall ein Zugriff auf die Daten der Kunden erforderlich ist, müsse explizit eine Freischaltung vom Kunden erfolgen. Zum Zeitpunkt meines Besuches war hierzu jedoch weder ein Hinweis in den AGBs noch in den Datenschutzhinweisen enthalten. Dies war nachzubessern.

Zugleich waren auch die übersandten Datenschutzerklärungen für die Nutzer des Angebotes nicht ausreichend. Insbesondere der Standardtext der Datenschutzerklärung der Online-Terminbuchung ließ wesentliche Informationen vermissen. So wurden dort keine Aussagen zum Ort der Speicherung sowie zur Dauer der Speicherung getroffen. Unerwähnt blieb auch, in welchen Konstellationen Terminland die Daten einsehen kann. Auf mein Betreiben hin wurden daher die mir zur Verfügung gestellten Texte überarbeitet.

Bemängelt habe ich schließlich auch, dass die Hinweise zum Datenschutz bei den von mir geprüften Internetangeboten nicht der Datenerhebung vorgeschaltet waren. Hier ist dafür Sorge zu tragen, dass der Nutzer die Informationen vor der Eingabe seiner persönlichen Daten zur Kenntnis nehmen kann.

b) Fehlende Transparenz auf der Homepage der Kunden

Bei der Nutzung von Terminland über die Internetangebote von diversen Arztpraxen ist mir im Übrigen aufgefallen, dass es in einigen Fällen nicht klar für den Nutzer erkennbar ist, dass er nunmehr bei der angestrebten Terminvereinbarung ein Angebot von Terminland nutzt. So gibt es beispielsweise die Variante, dass der Nutzer über einen Link auf die Seite von Terminland weitergeleitet wird. Zugleich haben jedoch manche Ärzte das Terminlandangebot so in ihre Homepage integriert, dass für den Anwender nicht klar erkennbar ist, dass nunmehr das Angebot eines externen Anbieters genutzt wird. Zumeist findet sich lediglich in kleiner Schrift der knappe Hinweis „Ein Service von Terminland.de“. Eine dritte Variante beinhaltet letztlich die Möglichkeit, dass sich eine Arztpraxis beider Varianten bedient.

Aus meiner Sicht ist hier nur die erste Variante ein gangbarer Weg. Bei der zweiten Variante müsste Terminland sicherstellen, dass der Vertragspartner auf seiner Homepage klar erkennbar hervorhebt, dass das Angebot über einen externen Anbieter gesteuert wird.

Der Datenschutzbeauftragte von Terminland merkte mir gegenüber an, dass er nach seiner Prüfung keine Möglichkeit sieht, die Vertragspartner zu einem entsprechenden Vorgehen zu verpflichten. Letztlich sei die Ausgestaltung der Homepage im Verantwortungsbereich der Ärzte gelegen. Es wurde daher vereinbart, dass die Vertragspartner mit einem entsprechenden Hinweisblatt über die Sachlage informiert werden. Zugleich habe ich darauf hingewiesen, dass etwaige Verstöße gegen die vorgegebene Verfahrensweise künftig gegebenenfalls gegenüber der verantwortlichen Stelle geahndet werden müssen. Auch dies wurde in das vereinbarte Hinweisblatt aufgenommen.

c) Umfang der Informationen in den E-Mails zur Terminbestätigung

Zum Schluss hat sich für mich auch noch einmal die Frage gestellt, in welcher Form und mit welchem Inhalt Terminbestätigungen per E-Mail an die Nutzer von Terminland zu senden sind.

Wie mir mitgeteilt wurde, besteht für den Kunden die Möglichkeit, eine Terminbestätigung per E-Mail zu deaktivieren. Da auch diese Einstellung im Verantwortungsbereich der Kunden von Terminland liegt, wurde vereinbart, auch hierzu die Kunden noch einmal ausdrücklich in einem Merkblatt darüber zu informieren, dass entsprechende Terminbestätigungen in der Regel nur die erforderlichen Angaben enthalten sollten, da ein unverschlüsselter E-Mail-Versand erfolgt.

In der Regel ist nicht erforderlich, die Diagnose und den Behandlungsgrund in der Terminbestätigung aufzuführen. Auch die Erforderlichkeit des kompletten Geburtsdatums und der Anschrift des Patienten war nicht nachvollziehbar. Wie man mir diesbezüglich mitteilte, besteht letztlich auch die Möglichkeit, entsprechende Angaben in verkürzter Form abzubilden (indem etwa einzelne Buchstaben oder Zahlen mit einem „Sternchen“ ausgeblendet werden).

Ausblick

Wie aus einer Umfrage aus dem Jahr 2017 hervorgeht, steht die Bevölkerung digitalen Gesundheitsangeboten grundsätzlich positiv gegenüber. Entsprechende Angebote, wie das von Terminland, sind insoweit aus dem täglichen Alltag nicht mehr wegzudenken. Gemäß der genannten Umfrage vereinbaren bereits 18 % der Befragten Termine online mit dem Arzt; 40 % würden es gerne tun, wenn es das Angebot geben würde. Bei entsprechenden Angeboten ist jedoch im Verhältnis zum Nutzen immer darauf zu achten, dass bei so sensiblen Daten wie den eigenen Gesundheitsdaten auch der Schutz der Daten angemessen gewährleistet bleibt.

7.6
Das neue Transplantationsregistergesetz

Im Hinblick auf das neue Transplantationsregistergesetz hat sich herausgestellt, dass die Stellen, die im Rahmen einer Einwilligung Daten von Patienten erhalten sollen (Registerstelle und Vertrauensstelle), derzeit noch nicht feststehen. Diesbezüglich wurde mir gegenüber geltend gemacht, dass hier das Vorliegen einer informierten Einwilligung angezweifelt werden könne, da der Patient nicht wisse, wo genau seine Daten verarbeitet werden. In der Angelegenheit wurde von mir ein Länderaustausch initiiert und eine Ergänzung zur Einwilligungserklärung entworfen, die diesem Umstand Rechnung trägt.

Anlass

In einer Anfrage des Datenschutzbeauftragten eines Universitätsklinikums wurde ich darauf hingewiesen, dass gemäß dem „Gesetz zur Errichtung eines Transplantationsregisters und zur Änderung weiterer Gesetze“ künftig mittels einer Einwilligungserklärung der Deutschen Krankenhausgesellschaft die Einwilligung zur Datenübermittlung an ein entsprechendes Transplantationsregister einschließlich einer Vertrauensstelle einzuholen ist. Stand jetzt ist aber, dass aufgrund eines noch nicht abgeschlossenen Ausschreibungsverfahrens noch nicht geklärt ist, welche Stellen künftig diese Aufgaben ausführen werden. Der Datenschutzbeauftragte des Klinikums hat deshalb angefragt, ob diesem Umstand mit einer „Ergänzung zur Patienteninformation gemäß § 15e Transplantationsgesetz (TPG) für die Datenübermittlung an die Transplantationsregisterstelle und die Vertrauensstelle“ Rechnung getragen werden kann, so dass im Endeffekt von einer informierten Einwilligung auszugehen ist. Die übersandte Ergänzung enthielt u. a. den folgenden Text:

> *„Sehr geehrte Patientin, sehr geehrter Patient,*
> *in der Ihnen überreichten, oben benannten Patienteninformation haben wir Ihnen mitgeteilt, dass zum heutigen Zeitpunkt noch nicht feststeht, welche Einrichtung mit der Aufgabe der Führung des Transplantationsregisters und welche Einrichtung mit der Führung der Vertrauensstelle beauftragt werden, und dass wir als Transplantationszentrum allerdings bereits heute dazu verpflichtet sind, Sie darüber aufzuklären und auch Ihre diesbezügliche Einwilligung in die Übermittlung einzuholen.*
> *Um Ihnen diese noch ausstehende Information zukünftig zur Verfügung zu stellen, haben Sie die Möglichkeit, sich im Internet unter der Adresse*
> *http:\\www.muster.de*

über den Stand der konkreten Ausgestaltung dieser Einrichtung zu informieren. Solange diese Einrichtungen noch nicht etabliert sind, finden Sie auf dieser Webseite einen entsprechenden diesbezüglichen Hinweis. Sobald diese Einrichtungen aber etabliert sind, finden Sie auf dieser Webseite unverzüglich, und dann für den Zeitraum eines Jahres, die konkreten Informationen, welche Einrichtung mit der Aufgabe der Führung des Transplantationsregisters und welche Einrichtung mit der Führung der Vertrauensstelle beauftragt wurden. Sie haben aber auch die Möglichkeit, eine Einwilligung erst dann zu erteilen, wenn die oben genannten Einrichtungen feststehen.
Sollten Sie hierzu noch Fragen haben, sprechen Sie die Mitarbeiterin/den Mitarbeiter unseres Universitätsklinikums, die/der Ihnen diese Information ausgehändigt hat, gerne dazu an."

Wie mir ergänzend hierzu vom zuständigen Datenschutzbeauftragten mitgeteilt wurde, falle, wenn die Einwilligungen nicht kontinuierlich eingeholt werden, ein erheblicher, nachträglicher Meldeaufwand beim Transplantationszentrum an. So bestehe etwa das kaum leistbare Erfordernis der nachträglichen Patienteninformation mit dem Einholen der Einwilligung. Beispielhaft wurde mir dabei der Bereich der Nierentransplantation genannt, bei dem alleine im relevanten Zeitraum an die 800 Patienten betroffen sein können.

Datenschutzrechtliche Bewertung und getroffene Maßnahmen

Da sich die aufgezeigte Problematik bundesweit stellte, habe ich diesbezüglich auch noch einmal meine Länderkollegen kontaktiert. Im Ergebnis haben mir die Kollegen von zwei Ländern mitgeteilt, dass sie keine datenschutzrechtlichen Bedenken haben, sofern die zitierte Ergänzung zur Patienteninformation zum Einsatz kommt. Nach Art. 13 Abs. 1 lit. e DS-GVO ist die betroffene Person „gegebenenfalls (über) die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten" zu informieren. Auch wenn in dieser Regelung die Informationspflichten und nicht die Voraussetzungen für eine informierte Einwilligung festgelegt werden, ist davon auszugehen, dass eine Person, die diese Informationen erhält, als darüber informiert im Sinne der DS-GVO gilt. Wenn mithin bereits die Angabe von „Kategorien" von Empfängern ausreichend ist, und dies insbesondere dann, wenn eine konkrete Angabe des Empfängers zum aktuellen Zeitpunkt noch nicht möglich ist, sind mit der Ergänzung zur Patienteninformation die Voraussetzungen für eine informierte Einwilligung in die Datenübermittlung gegeben.

Auch ich habe mich dieser Auffassung angeschlossen.

Ich habe die Hessische Krankenhausgesellschaft gleichermaßen noch einmal darum gebeten, ihre Mitglieder auf diese Problematik hinzuweisen, wobei dabei auch das zitierte Muster Verwendung finden kann. Nach meinem letzten Kenntnisstand wurde meine Mitteilung zwischenzeitlich auch an die Deutsche Krankenhausgesellschaft weitergeleitet, die sich insoweit ihrerseits noch einmal mit der Thematik beschäftigen wollte. Beim eingebenden Universitätsklinikum kommt das abgestimmte Formular mittlerweile zur Anwendung.

7.7
Prüfung eines Unternehmens aus dem Bereich Markt- und Meinungsforschung

Auch für Unternehmen im Bereich der Markt- und Meinungsforschung gilt, dass die im Unternehmen aufbewahrten Daten von Personal oder Dritten vor einem unbefugten Zugriff zu sichern sind. Es sind insoweit entsprechende technisch-organisatorische Maßnahmen vorzusehen.

Der Anlass

Eine ehemalige Mitarbeiterin eines Markt- und Meinungsforschungsunternehmens aus dem Raum Frankfurt berichtete mir, sie habe bei ihrer Tätigkeit dort miterleben müssen, dass datenschutzrechtliche Vorgaben nur bedingt beachtet würden. So seien etwa Blätter mit vertraulichen Daten intern nur unzureichend gesichert gewesen und zum Teil als Schmierpapier verwendet worden. Der Aktenvernichter im Haus werde offenbar nur selten benutzt und auch eine Datenschutztonne habe sie nie gesehen. Darüber hinaus seien Daten der Marktforschungsteilnehmer weiterhin im System aufbewahrt worden, obwohl eine Löschung zugesagt worden sei.

Die größten Missstände seien im Callcenter-Raum aufgetreten. Dort seien teils wichtige Dokumente mit vertraulichen Teilnehmerdaten für jedermann zugänglich in den Schränken im hinteren Bereich des Raumes aufbewahrt worden. In den dortigen Schnellheftern/Ordnern hätten sich auch Namen von Ärzten und Krankenhäusern befunden, die in der Vergangenheit an Studien teilgenommen hatten.

Vorgefundene Situation beim Ortstermin

Soweit dies die Schrankwand im Callcenter-Raum betrifft, konnte tatsächlich festgestellt werden, dass in den nicht abschließbaren Schränken zum Teil sensible Daten in Aktenordnern aufgehoben werden. Darunter befanden sich neben Akten aus dem Bereich Steuern auch Akten aus dem Personalbereich, die Angaben zum Lohn der Mitarbeiter enthielten.

Bei dem Besuch konnte zudem festgestellt werden, dass der zuständige IT-Leiter des Unternehmens auch die Stellung als Datenschutzbeauftragter des Unternehmens innehat. Mit dieser doppelten Funktion geht jedoch regelmäßig ein zu befürchtender Interessenkonflikt einher.

Des Weiteren wurde festgestellt, dass in dem Haus keine konkreten Löschfristen für die Vernichtung von Daten aus abgeschlossenen Projekten vorgesehen sind.

Die übrigen von der Eingebenden gemachten Vorwürfe konnten bei dem Besuch nicht bestätigt werden.

Ergebnis und getroffene Maßnahmen

Hinsichtlich der Schrankwand im Callcenter-Raum habe ich dem Unternehmen aufgegeben, dass diese mit entsprechenden Vorrichtungen zu versehen ist, die einen unbefugten Zugriff verhindern. Dies gilt gleichermaßen auch für die übrigen Schränke mit sensitiven/personenbezogenen Daten in dem Betrieb.

Soweit dies die Person des Datenschutzbeauftragten und den damit in dieser Konstellation einhergehenden, drohenden Interessenkonflikt betrifft, habe ich noch einmal auf mein Merkblatt zum betrieblichen Datenschutzbeauftragten verwiesen. Zwischenzeitlich wurde die Stelle des Datenschutzbeauftragten von dem geprüften Unternehmen an einen externen Datenschutzbeauftragten vergeben. Dieser hat mittlerweile auch konkrete Löschfristen ausgearbeitet und mir ein entsprechendes Konzept zukommen lassen.

Im Rahmen der vertraglichen Aufbewahrungs- bzw. Nachweispflichten nach Durchführung der Befragung nicht mehr benötigte personenbezogene Daten (z. B. Adress- oder Kontaktdaten) werden künftig bei Abschluss der Auswertung, d. h. spätestens nach einem Jahr, gelöscht.

Eine Überarbeitung bedurfte im Übrigen auch nochmal die Anmeldung nach § 4d BDSG zum Register nach § 38 Abs. 2 BDSG, da mir noch veraltete Daten des Unternehmens gemeldet waren.

8. Sozialwesen

8.1
Datenübermittlung eines kommunalen Jobcenters bei polizeilichem Auskunftsersuchen in einem Verfahren mit Tötungsdelikt

Grundsätzlich richtet sich die Möglichkeit und Zulässigkeit einer Sozialdatenübermittlung bei Auskunftsersuchen von Polizeibehörden nach § 68 SGB X oder nach § 73 SGB X. Eine auf § 73 SGB X gestützte Auskunft eines kommunalen Jobcenters an eine Polizeibehörde ohne vorliegende richterliche Anordnung ist gesetzlich ausgeschlossen. In besonderen, speziell gelagerten polizeilichen Einzelfällen, in deren Zusammenhang eine Sozialdatenübermittlung sinnvoll erscheint, kann und muss das kommunale Jobcenter darauf hinwirken, dass sich die ermittelnde Polizeibehörde eine richterliche Anordnung einholt, um rechtskonform Sozialdaten übermitteln zu können.

Ein hessisches kommunales Jobcenter wandte sich an mich, weil dieses ein spezielles Auskunftsersuchen der Polizei erreicht hatte. Die Polizei schilderte in ihrem Auskunftsersuchen, dass sie umfangreich Ermittlungen in einem Tötungsdelikt in Hessen durchführe, in deren Rahmen eine tot aufgefundene weibliche Person trotz umfangreicher Ermittlungen und Nachforschungen sowie einer Öffentlichkeitsfahndung über viele Monate hinweg nicht identifiziert werden konnte. Die Ermittlungen hatten bislang ergeben, dass das Opfer in der Nähe des Fundortes gewohnt haben müsse, zwischen 40 und 65 Jahre alt gewesen sein und einen Geburtsort außerhalb Deutschlands haben dürfte. Da die Polizei u. a. auch keine Vermisstenanzeige eines möglichen Arbeitgebers erreicht hatte, erschien es möglich, dass die Tote womöglich Sozialleistungsempfängerin gewesen sein könnte.

Mit diesem Hintergrund wandte sich die Polizei an das kommunale Jobcenter des Landkreises, in dem sich der Fundort befand, und bat dieses um eine Auskunft über alle weibliche Personen,

– die bis mindestens in das Jahr 2016 in einem von zwei dem Fundort am nächsten liegenden Stadtteilen des Fundortes der Toten gewohnt haben oder noch wohnen,
– deren Geburtsort sich außerhalb Deutschlands befindet und
– deren Alter zwischen 40 und 65 Jahren liegt.

Die Polizei versprach sich von dieser gewünschten Liste, bei ihren Ermittlungen nach dem Ausschlussprinzip voranzukommen und eine Frau als die Tote verifizieren zu können.

Für dieses „Massen-Auskunftsersuchen“ gab die Polizei dem kommunalen Jobcenter keine Rechtsgrundlage an, auf die sie sich stützte. Das kommunale Jobcenter nahm diesen speziellen Sachverhalt aber zum Anlass, die Zulässigkeit der von der Polizei gewünschten Sozialdatenübermittlung zu prüfen und suchte hierfür den Kontakt zu mir.

Das kommunale Jobcenter hatte § 68 SGB X als mögliche Übermittlungsbefugnis zutreffend ausgeschlossen, da § 68 Abs. 1 SGB X ausdrücklich einen einzelnen Leistungsfall des Sozialleistungsträgers adressiert.

§ 68 Abs. 1 SGB X

Zur Erfüllung von Aufgaben der Polizeibehörden, der Staatsanwaltschaften und Gerichte, der Behörden der Gefahrenabwehr und der Justizvollzugsanstalten dürfen im Einzelfall auf Ersuchen Name, Vorname, Geburtsdatum, Geburtsort, derzeitige Anschrift des Betroffenen, sein derzeitiger oder zukünftiger Aufenthaltsort sowie Namen, Vornamen oder Firma und Anschriften seiner derzeitigen Arbeitgeber übermittelt werden, soweit kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden, und wenn das Ersuchen nicht länger als sechs Monate zurückliegt. Die ersuchte Stelle ist über § 4 Abs. 3 hinaus zur Übermittlung auch dann nicht verpflichtet, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann. Satz 2 findet keine Anwendung, wenn das Amtshilfeersuchen zur Durchführung einer Vollstreckung nach § 66 erforderlich ist.

Da eine richterliche Anordnung i. S. d. § 73 Abs. 3 SGB X

§ 73 SGB X

(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich ist.

(2) Eine Übermittlung von Sozialdaten zur Durchführung eines Strafverfahrens wegen einer anderen Straftat ist zulässig, soweit die Übermittlung auf die in § 72 Abs. 1 Satz 2 genannten Angaben und die Angaben über erbrachte oder demnächst zu erbringende Geldleistungen beschränkt ist.

(3) Die Übermittlung nach den Absätzen 1 und 2 ordnet der Richter an.

nicht vorlag, zog das kommunale Jobcenter bei seiner Prüfung zunächst auch § 69 Abs. 1 Nr. 1, 2. Alt. SGB X in Erwägung.

§ 69 Abs. 1 Nr. 1 SGB X

Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist

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

Diese Erwägung beruhte auf der möglichen Fallkonstellation, dass die Sozialdatenübermittlung seitens des kommunalen Jobcenters zur Verifizierung der (fort-)bestehenden Leistungsberechtigung einer (bisher) dort im Leistungsbezug stehenden Person und damit zur Erfüllung einer eigenen Aufgabe erforderlich sein könnte, nämlich ob ein Leistungsanspruch weiter besteht oder erloschen sein könnte.

In dem fachlichen Austausch zwischen dem behördlichen Datenschutzbeauftragten des kommunalen Jobcenters und mir wurde ein dem sensiblen Auskunftsersuchen angemessener rechtlicher Weg gesucht. Auch wenn ich eine Übermittlung auf Grundlage von § 69 Abs. 1 Nr. 1, 2. Alt. SGB X nicht für gänzlich ausgeschlossen hielt, habe ich den Weg über eine richterliche Anordnung gemäß § 73 SGB X favorisiert.

Ich habe das kommunale Jobcenter gebeten, die Polizei über diese Vorschrift zu informieren und diese darum zu bitten, sich um eine richterliche Anordnung zu bemühen. Diese richterliche Anordnung erreichte das kommunale Jobcenter kurze Zeit später. Auf dieser Rechtsgrundlage übermittelte das kommunale Jobcenter im Ergebnis Daten im geringstmöglichen Umfang von 26 weiblichen Personen an die Polizei.

8.2
Dauerbrenner: Foto- und Videoaufnahmen von Kindern in Kindertageseinrichtungen

In Kindertageseinrichtungen besteht aus unterschiedlichen Gründen der Wunsch, Foto- und Videoaufnahmen sowie Tonaufzeichnungen von innerhalb der Einrichtung betreuten Kindern

zu machen. In diesen Fällen ist das Recht der Kinder am eigenen Bild und Wort in Verbindung mit dem elterlichen Sorgerecht zu beachten.

Mit der Thematik befasste ich mich bereits in meinem 42. Tätigkeitsbericht (Ziff. 3.3.7.6). Auch im gegenwärtigen Berichtszeitraum erreichten mich wieder Anfragen von Kindertageseinrichtungen und Sorgeberechtigten betroffener Kinder. Gefragt wurde, in welchem Rahmen es datenschutzrechtlich zulässig sei, Foto- oder Videoaufnahmen von Kindern während ihrer Aufenthaltszeit in einer Einrichtung, z. B. in Spielsituationen, zu machen. Mehrfach wandten sich Sorgeberechtigte auch erst im Nachgang bereits seitens der Einrichtung gefertigter Fotos an mich und teilten mit, von Fotoaufnahmen hätten sie nichts gewusst und mit solchen, ungefragt, auch nicht gerechnet.

Die rechtliche Würdigung findet sich bereits in dem erwähnten Beitrag „Videoaufnahmen von Kindern im Kindergarten oder in einer Kindertagesstätte“ in meinem 42. Tätigkeitsbericht.

Subjektive Rechte wie das „Recht am eigenen Bild“ oder das „Recht am gesprochenen Wort“ spiegeln, abgeleitet aus dem Persönlichkeitsrechtsschutz, den Anspruch des Einzelnen auf informationelle Selbstbestimmung bei Erhebungen und Verwendungen seine Person betreffender Daten und Informationen wider.

Das „Recht am eigenen Bild“ schützt vor jeder Art der unbefugten Anfertigung, Verbreitung oder Veröffentlichung einer bildlichen Darstellung seiner Person durch stoffliche Fixierung und z. B. auch vor der mittels technischer Geräte bewirkten Direktübertragung seines Erscheinungsbildes. Auch hinsichtlich der Herstellung und Verbreitung des Bildes steht Betroffenen ein Selbstbestimmungsrecht zu, nach dem nur sie selbst darüber zu befinden haben, ob und wie sie sich in der Öffentlichkeit oder gegenüber Dritten darstellen und wer diese Daten speichert, nutzt und übermittelt.

Bereits in meinem 36. Tätigkeitsbericht (Ziff. 5.6.4, „Datenschutzfragen bei der Erstellung und Behandlung von Schülerfotos“; zu finden z. B. im Internet auf meiner Homepage unter www.datenschutz.hessen.de), habe ich festgestellt, dass eine Schule kein Recht am Bild der Schülerinnen und Schüler besitzt und diese auch nicht die Pflicht haben, ein Foto zu dulden. Diese Einschätzung ist auf Anfragen von Kindertageseinrichtungen entsprechend übertragbar.

Seine Grundlagen hat das Recht am eigenen Bild im Persönlichkeitsrecht der Art. 1 Abs. 1 und 2 Abs. 1 GG, in §§ 22, 23 KunstUrhG i. V. m. § 33 KunstUrhG und in § 201a StGB.

Das Recht am eigenen Bild ist hinsichtlich der unbefugten Verarbeitung bzw. Veröffentlichung des Bildes einer Person strafrechtlich durch § 33 KunstUrhG geschützt, der ein in § 22 KunstUrhG enthaltenes Verbot sanktioniert. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder zur Schau gestellt werden (§ 22 Abs. 1 KunstUrhG), wobei unter Bildnis – unabhängig vom eingesetzten Verfahren – jede Wiedergabe des äußeren Erscheinungsbildes einer identifizierbaren Person zu verstehen ist.

Eltern bzw. Sorgeberechtigte müssen also in jedem Fall zwingend eine informierte, transparente und freiwillige Einwilligung für die Anfertigung eines/von Fotos ihres eigenen Kindes vorab schriftlich erklärt haben. Wenn die Eltern bzw. Sorgeberechtigten ihre erforderliche schriftliche Einwilligung verweigern oder nur in einem konkret beschriebenen Rahmen abgeben, hat sich die angesprochene Stelle daran zwingend zu halten, da sie andernfalls gegen § 22 Abs. 2 KunstUrhG verstößt.

Eine solche Einwilligung kann im Übrigen nie für „fremde“ Kinder erklärt werden, da das oben angesprochene allgemeine Persönlichkeitsrecht eine höchstpersönliche Angelegenheit ist.

Grundsätzlich sehe ich aber auch die Gestaltung eines hinreichend präzisen Einwilligungstextes als schwierig an. Eine „Pauschal-Einverständniserklärung“ für die Aufnahme von Fotos und/oder Filmen für die Dauer der Zugehörigkeit eines Kindes in der Kindertageseinrichtung halte ich für zu unbestimmt und global – eine erforderliche „informierte“ Einwilligung wäre den Eltern so nicht möglich. Hier bleibt die verantwortliche Stelle, also die jeweilige Kindertageseinrichtung, gefordert, eine adäquate, auf den jeweiligen Sinn und Zweck ausgerichtete Formulierung zu finden.

8.3
Aufbewahrungsfrist von Sozialakten in kommunalen Jobcentern

Aus dem Zweckbindungsgrundsatz folgt, dass für Sozialdaten eine begrenzte Aufbewahrungsfrist besteht. Die Aufbewahrung ist damit aus der Natur der Sache befristet.
Das Sozialgesetzbuch sieht jedoch weder im den Sozialdatenschutz regelnden SGB X noch im SGB II konkrete Aufbewahrungsfristen für Sozialakten in kommunalen Jobcentern vor.

Der Hessische Landkreistag wollte für die hessischen kommunalen Jobcenter eine Orientierungs- und Arbeitshilfe zur dortigen Wahrung und Umsetzung sozialdatenschutzrechtlicher Vorgaben erarbeiten. In diesem Zusammenhang tauchte während der Ausarbeitung die Frage

nach Aufbewahrungsfristen der Akten in den kommunalen Jobcentern auf. Der Hessische Landkreistag wandte sich hierzu an mich mit der Bitte um meine datenschutzrechtliche Einschätzung und Stellungnahme.

Hinsichtlich der Bestimmung der Aufbewahrungsfristen von Akten im Bereich des SGB II ist maßgeblicher Ausgangspunkt § 84 Abs. 2 SGB X, wonach Sozialdaten zu löschen sind, wenn diese für die Aufgabenerfüllung nicht mehr benötigt werden.

§ 84 Abs. 2 SGB X

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

Doch auch nach dem eigentlichen Bearbeitungsende, dem Schließen der Akte, kann noch eine Erforderlichkeit der Speicherung bestehen, wenn sich diese aus gesetzlichen Vorgaben ergibt, die sich auf den Zeitpunkt der Aussonderung der Akten auswirken.

Regelungen auf Bundesebene

Die Bundesagentur für Arbeit legt auf Bundesebene für Akten mit Standardfällen eine Aufbewahrungsfrist von fünf Jahren zugrunde, welche sich aus den für das Haushalts-, Kassen- und Rechnungswesen des Bundes (ABestB – HKR) niedergelegten Aufbewahrungsbestimmungen ergibt (vgl. Bundesagentur für Arbeit, Zentrale, PEG 23 – II – 5020 / II- 5001 mit Stand März 2013, Hinweise zum Aufbau und Führen einer Leistungsakte & verbindliche Regelungen zu den Aufbewahrungsfristen im Rechtskreis SGB II).

Regelung auf Länderebene

a) Akten mit zahlungsbegründenden Unterlagen

Auf der Länderebene in Hessen ergibt sich aus § 37 GemHVO, der die Aufbewahrung von Unterlagen und Aufbewahrungsfristen regelt, allerdings eine Frist von zehn Jahren.

§ 37 GemHVO

(1) Die Bücher und Belege sind sicher aufzubewahren. Soweit begründende Unterlagen nicht den Kassenanordnungen beigefügt sind, obliegt ihre Aufbewahrung den anordnenden Stellen.

(2) Der Jahresabschluss ist in ausgedruckter Form dauernd aufzubewahren. Die Bücher und Inventare sind zehn Jahre, die Belege sechs Jahre aufzubewahren. Ergeben sich Zahlungsgrund und Zahlungspflichtige oder Empfangsberechtigte nicht aus den Büchern, sind die Belege so lange wie die Bücher aufzubewahren. Gutschriften, Lastschriften und die Kontoauszüge der Kreditinstitute sind wie Belege aufzubewahren. Die Fristen beginnen am 1. Januar des der Beschlussfassung über den Jahresabschluss (§ 114 Abs. 1 der Hessischen Gemeindeordnung) folgenden Haushaltsjahres.

(3) Nach Ablauf von drei Jahren seit Beginn der Aufbewahrungsfrist können die Bücher, Inventare und Belege auf Bild- oder Datenträgern aufbewahrt werden, wenn sichergestellt ist, dass der Inhalt der Bild- oder Datenträger mit den Originalen übereinstimmt und jederzeit lesbar gemacht werden kann. Die Bild- oder Datenträger sind nach Abs. 1 und 2 anstelle der Originale aufzubewahren.

Der Bürgermeister kann zulassen, dass der Inhalt von Büchern und Belegen vor Ablauf der in Satz 1 genannten Frist auf Bild- oder Datenträger übernommen wird, wenn sichergestellt ist, dass die Daten innerhalb der Frist jederzeit in ausgedruckter Form lesbar gemacht werden können. Bei Betrieben gewerblicher Art ist § 147 der Abgabenordnung, zuletzt geändert durch Gesetz vom 26. Juli 2016 (BGBl. I S. 1824), zu beachten.

(4) Werden automatisierte Verfahren, in denen Bücher und Belege gespeichert sind, geändert oder durch andere Verfahren ersetzt, muss die maschinelle Auswertung der gespeicherten Daten innerhalb der Aufbewahrungsfristen auch mit den geänderten oder neuen Verfahren oder durch ein anderes System gewährleistet sein.

Die Vorschrift hat als lex specialis Vorrang vor den Bestimmungen des Hessischen Aktenführungserlasses. § 37 Abs. 1 GemHVO legt zunächst fest, dass Bücher und Belege sicher und geordnet aufzubewahren sind. Soweit begründende Unterlagen nicht den Kassenanordnungen beigefügt sind, obliegt ihre Aufbewahrung den anordnenden Stellen.

Als begründende Unterlagen sind alle Schriftstücke zu qualifizieren, die eine Kassenanordnung oder die Buchung aufgrund allgemeiner Kassenanordnung begründen (zur Definition vgl.

auch o. g. Schreiben der Bundesagentur für Arbeit, Punkt 5.1). Damit erfasst die Norm als solche zahlungsbegründenden Unterlagen insbesondere alle Anträge, mit denen Leistungen nach dem SGB II geltend gemacht werden, sowie alle eingereichten Unterlagen und Bescheinigungen, die zur Mitteilung oder zum Nachweis von Angaben dienen, die Einfluss auf die Ermittlung und Auszahlung eines Leistungsanspruchs haben.

Die Frist selbst ergibt sich aus Absatz 2 der Norm, welcher bestimmt, dass der Jahresabschluss in ausgedruckter Form dauernd aufzubewahren ist. Die Bücher und Inventare sind zehn Jahre, die Belege sechs Jahre aufzubewahren. Ergeben sich Zahlungsgrund und Zahlungspflichtige oder Empfangsberechtigte nicht aus den Büchern, sind die Belege so lange wie die Bücher aufzubewahren. Gutschriften, Lastschriften und die Kontoauszüge der Kreditinstitute sind wie Belege aufzubewahren. Die Fristen beginnen am 1. Januar des der Beschlussfassung über den Jahresabschluss (§ 114 Abs. 1 HGO) folgenden Haushaltsjahres.

Es ergibt sich daraus zunächst Folgendes:

Akten sind ab 1. Januar des der Beschlussfassung über die Jahresrechnung folgenden Haushaltsjahres grundsätzlich zehn Jahre aufzubewahren.

Die Zeitpunkte für den Abschluss der Bearbeitung einer Akte, welche für die anschließende Fristberechnung maßgeblich sind, sind – in Anlehnung an die Ansätze der Bundesagentur für Arbeit sowie an die Vorgaben des Hessischen Aktenführungserlasses – wie nachfolgend aufgeführt zu bestimmen:

– Für alle eine Leistung beinhaltenden Fälle ist der für die Fristberechnung maßgebliche Zeitpunkt der der letzten Auszahlung.
– Bei bestehenden Forderungen (z. B. bei Darlehen, Rückforderungen, Erstattungsansprüchen usw.) ist maßgeblicher Bezugspunkt für die Fristberechnung nach § 37 GemHVO der Eingang der letzten Einnahme.
– Bei Fehlbeträgen ist maßgeblicher Bezugspunkt für den Lauf der Frist der Abschluss der Bearbeitung.
– Für medizinische Unterlagen ergibt sich analog § 304 Abs. 1 Satz 1 i. V. m. § 292 SGB V ebenfalls eine Frist von zehn Jahren.

b) Akten ohne zahlungsbegründende Unterlagen

Abweichungen von diesem Grundsatz ergeben sich dann, wenn keine Zahlungen bewirkt wurden. Für Dokumente, Vorgänge und Akten, die also nicht in den Bereich der zahlungsbegründenden Unterlagen fallen, ergeben sich die Aufbewahrungsfristen aus dem Hessischen Aktenführungserlass.

Nach dessen Anlage B (zu Nr. 11) ist für alle Akten und Vorgänge, für die keine besondere Aufbewahrungsfrist festgesetzt ist, von einer Frist von fünf Jahren auszugehen (Abs. 6, Punkt B 5). Eine Verkürzung der Frist auf ein Jahr ist dann vorzunehmen, wenn Vorgänge ihrer Bedeutung nach keiner längeren Aufbewahrung bedürfen (Abs. 6, Punkt B 6).

Hinsichtlich der Bestimmung des Beginns der Aufbewahrungsfrist gilt für Akten, in denen keine Leistung gewährt wurde und diese mit Verwaltungsakt abgelehnt wurde, dass dieser Zeitpunkt maßgeblich ist. Die Aufbewahrungsfrist beginnt dann mit dem Schluss des Kalenderjahres, in dem die Akte, der Vorgang, die Liste oder das Buch abgeschlossen worden ist [Anlage B (zu Nr. 11), Abs. 5]. Dieser Beginn ist ebenfalls zugrunde zu legen für sonstige Vorgänge ohne Leistungsgewährung und ohne Bescheiderteilung.

Es ist darauf hinzuweisen, dass sich für bestimmte Unterlagen wie etwa Urkunden über Rechte an Grundstücken oder gerichtliche Schuldtitel längere Fristen ergeben können.

c) Digitalisierung

Hinzuweisen ist auch auf § 37 Abs. 3 GemHVO, wonach nach Ablauf von drei Jahren seit Beginn der Aufbewahrungsfrist die Bücher, Inventare und Belege auf Bild- oder Datenträgern aufbewahrt werden können, wenn sichergestellt ist, dass der Inhalt der Bild- oder Datenträger mit den Originalen übereinstimmt und jederzeit lesbar gemacht werden kann. Die Bild- oder Datenträger sind nach Abs. 1 und 2 anstelle der Originale aufzubewahren.

Nach dieser Vorschrift kann der Bürgermeister (bzw. vorliegend die verantwortliche Person im Jobcenter) zulassen, dass der Inhalt von Büchern und Belegen vor Ablauf der in Satz 1 genannten Frist auf Bild- oder Datenträger übernommen wird, wenn sichergestellt ist, dass die Daten innerhalb der Frist jederzeit in ausgedruckter Form lesbar gemacht werden können. Eine Digitalisierung der Akten kann demnach zu einer deutlich kürzeren Aufbewahrungsfrist der Papierakten (Lagerung) führen. Aus sozialdatenschutzrechtlicher Perspektive erscheint eine Aufbewahrungsdauer und -frist von in der Regel fünf Jahren (plus laufendes

(Haushalts-)Jahr) vertretbar und gegenüber zehn Jahren jedenfalls aus den allgemeinen datenschutzrechtlichen Grundsätzen der Datenvermeidung und Datensparsamkeit vorzugswürdig.

Wenn jedoch § 37 GemHVO – zu vertreten seitens der verantwortlichen Stellen – lückenlos Anwendung findet (vgl. Ausführungen zu dieser Vorschrift oben), so ist diese Vorschrift die zu beachtende Rechtsgrundlage, die die Aufbewahrungsdauer und -frist auf zehn Jahre ausdehnt.

Ergebnis

Der Hessische Landkreistag sieht für Hessen und dessen kommunale Jobcenter § 37 Abs. 2 GemHVO als maßgebliche Rechtsnorm an, woraus sich eine Aufbewahrungsfrist von zehn Jahren ergibt. Ich habe diese Entscheidung akzeptiert. Diese Frist hat der Hessische Landkreistag sodann in seine praktische Arbeitshilfe „Datenschutz und aufzubewahrende (digitale) Dokumente in den hessischen kommunalen Jobcentern“ als Vorgabe bzw. Empfehlung aufgenommen.

8.4
Adoptionsvermittlungsakten als Forschungsgegenstand

Adoptionsvermittlungsakten sind kein zulässiger Forschungsgegenstand, solange die adoptierte Person nicht ihren 100jährigen Geburtstag erreicht hat (erreicht hätte). Nach Ablauf dieser Frist richtet sich das weitere Verfahren nicht mehr nach dem Adoptionsvermittlungsgesetz, sondern nach dem Archivrecht der Länder.

Der Anlass

Das Hessische Ministerium für Soziales und Integration (HSM) ersuchte mich mit Blick auf ein angedachtes Forschungsprojekt um datenschutzrechtliche Beratung. Das HSM hielt das Projekt, bei dem es um die wissenschaftliche Auswertung von Adoptionsvermittlungsakten gehen sollte, wegen des Adoptionsvermittlungsgesetzes für unzulässig, während das Hessisches Ministerium für Wissenschaft und Kunst (HMWK) auf die Möglichkeit hinwies, das Forschungsvorhaben nach Maßgabe des Archivrechts zuzulassen.

Rechtliche Bewertung

Rechtssystematisch gehört das Adoptionsvermittlungsgesetz zum Sozialgesetzbuch (§ 68 Nr. 12 SGB I). Dies hat wiederum zur Folge, dass insbesondere auch der sogenannte Sozialdatenschutz gilt (§§ 67 ff. SGB X). Dieses Rechtsgebiet nimmt Rücksicht darauf, dass hier ein sensitiver Ausschnitt des Rechts auf informationelle Selbstbestimmung betroffen ist.

Nun hat nicht nur das Recht auf Datenschutz Grundrechtsqualität (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG), sondern auch die Forschung ist grundrechtsgeschützt (Art. 5 Abs. 3 GG). Es liegt auf der Hand, dass diese Grundrechtspositionen in ein Spannungsverhältnis geraten (können), wenn nämlich personenbezogene Daten zum Gegenstand eines Forschungsprojekts werden sollen. Dann müssen diese Grundrechte im konkreten Fall angemessen ausgeglichen werden (praktische Konkordanz). Dies ist im Sozialbereich das Anliegen des § 75 SGB X, der sich ausführlich mit der Übermittlung von Sozialdaten für die Forschung und Planung befasst.

Diese Norm verlangt mit Blick auf die Zulässigkeit von Forschungsvorhaben im Sozialbereich, dass schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt (§ 75 Abs. 1 S. 1 SGB X). Darüber in einem Genehmigungsverfahren zu entscheiden ist Aufgabe der jeweiligen obersten Landesbehörde, aus deren Bereich die zu übermittelnden Daten herrühren (§ 75 Abs. 2 SGB X), im Fall von Adoptionsvermittlungsakten, die ja Sozialdaten enthalten, also das Sozialministerium.

Mitunter reicht es für die sozialdatenschutzrechtliche Beurteilung allerdings nicht aus, sich auf die entsprechenden Normen im Zehnten Buch des Sozialgesetzbuchs zu beschränken, sondern das jeweilige Sozial-Fachgesetz weist zusätzlich spezifische Vorschriften auf, die dann das allgemeine Sozialdatenschutzrecht verdrängen. Dies ist bei dem Adoptionsvermittlungsgesetz der Fall.

Denn anders als im allgemeinen Sozialdatenschutzrecht ist hier die Verwendung von personenbezogenen Adoptionsvermittlungsdaten zugunsten der Forschung untersagt, § 9d AdVermiG.

§ 9d AdVermiG

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt das Zweite Kapitel des Zehnten Buches Sozialgesetzbuch mit der Maßgabe, dass Daten, die für Zwecke

dieses Gesetzes erhoben worden sind, nur für Zwecke der Adoptionsvermittlung oder Adoptionsbegleitung, der Anerkennung, Zulassung oder Beaufsichtigung von Adoptionsvermittlungsstellen, der Überwachung von Vermittlungsverboten, der Verfolgung von Verbrechen oder anderen Straftaten von erheblicher Bedeutung oder der internationalen Zusammenarbeit auf diesen Gebieten verarbeitet oder genutzt werden dürfen.

Da § 68 Nr. 12 SGB I, wie schon anfangs erwähnt, das Adoptionsvermittlungsgesetz dem Sozialgesetzbuch bereits zuordnet, ist der Verweis auf den Sozialdatenschutz (§§ 67 ff. SGB X) in § 9d AdVermiG an sich überflüssig. Rechtsgestaltend ist aber die enumerative Aufzählung der zulässigen Zwecke, für die Adoptionsdaten verwendet werden dürfen, und dass die Forschung, die an sich im Sozialdatenschutzrecht durch § 75 SGB X privilegiert ist, im Adoptionsvermittlungsrecht diese Rolle einbüßt. Dies hat zur Folge, dass Adoptionsvermittlungsakten erst dann der Forschung zugänglich sind, wenn sie nicht mehr dem Adoptionsvermittlungsgesetz unterliegen, sondern dem sich zeitlich anschließenden Archivrecht.

Damit stellt sich die Frage, wann dieser Zeitpunkt eintritt, also ab wann diese Akten nicht mehr im Bereich der Adoptionsverwaltung vorgehalten werden müssen.

Dies betrifft das Thema Aufbewahrungsfrist von Adoptionsvermittlungsakten, das in § 9b AdVermiG geregelt ist.

§ 9b AdVermiG

Aufzeichnungen und Unterlagen über jeden einzelnen Vermittlungsfall (Vermittlungsakten) sind, gerechnet vom Geburtsdatum des Kindes an, 100 Jahre aufzubewahren. Wird die Adoptionsvermittlungsstelle aufgelöst, so sind die Vermittlungsakten der Stelle, die ihre Aufgaben übernimmt, oder der zentralen Adoptionsstelle des Landesjugendamtes, in dessen Bereich die Adoptionsvermittlungsstelle ihren Sitz hatte, zur Aufbewahrung zu übergeben. Nach Ablauf des genannten Zeitraums sind die Vermittlungsakten zu vernichten.

Bevor die Akten vernichtet werden, müssen sie allerdings der Archivverwaltung angeboten werden; dies bestimmt sich nach dem jeweiligen Landesrecht.

Wenn die Archivverwaltung Akten wegen deren Archivwürdigkeit übernimmt, ist deren Nutzung für Forschungszwecke möglich. So bestimmt etwa § 14 HArchivG, dass die Nutzung von Archivgut einzuschränken oder zu versagen ist, wenn Grund zu der Annahme besteht, dass

schutzwürdige Belange Dritter beeinträchtigt werden. Das dürfte nach Ablauf der 100jährigen Frist im Adoptionsbereich regelmäßig nicht der Fall sein.

Über diese Rechtslage habe ich mich mit den beteiligten Ministerien verständigt. Das bedeutete zu diesem Zeitpunkt, dass Adoptionsvermittlungsakten ab Geburtsdatum 1917 und jünger für die Forschung noch tabu sind.

Die Frage, ob im Hinblick auf die steigende Lebenserwartung der deutschen Bevölkerung die Frist von 100 Jahren noch ausreicht, hat sich praktisch bislang noch nicht gestellt. Wichtiger erscheint mir allerdings der Hinweis, dass das Adoptionsvermittlungsgesetz die unter Grundrechtsschutz (Art. 5 Abs. 3 GG) stehende Forschungsfreiheit wohl verletzt, weil dieses Grundrecht in diesem Gesetz gänzlich unberücksichtigt geblieben, also gerade keine differenzierte, praktische Konkordanz herstellende Regelung getroffen worden ist.

8.5
Auftragsdatenverarbeitung in der Sozialverwaltung

Öffentliche Stellen müssen sich im Fall der Auftragsdatenverarbeitung nach dem Hessischen Datenschutzgesetz richten, während für nicht-öffentliche Stellen grundsätzlich das Bundesdatenschutzgesetz maßgebend ist. Hinzutreten können spezielle Vorschriften, etwa im Sozialrecht.

Der Anlass

Mehrfach erhielt ich Anfragen von öffentlichen und nicht-öffentlichen Stellen zu dem Thema Auftragsdatenverarbeitung. Nicht-öffentliche Stellen gehen dabei regelmäßig davon aus, dass der die Auftragsdatenverarbeitung betreffende § 11 BDSG anwendbar ist. Diese Annahme liegt nahe, weil das Bundesdatenschutzgesetz das datenschutzrechtliche Basisgesetz der Privatwirtschaft ist.

Rechtliche Bewertung

§ 11 BDSG gilt sowohl für die Bundesverwaltung als auch für die Privatwirtschaft. Wird jedoch ein Privatunternehmen für eine hessische öffentliche Stelle als Auftragnehmer tätig – und das

kommt sehr häufig vor –, ist § 11 BDSG nicht die entscheidende Rechtsvorschrift. Denn wenn hessische öffentliche Stellen personenbezogene Daten im Auftrag verarbeiten lassen, ist § 4 HDSG die maßgebende Regelung.

Allerdings liegt, wenn meine Behörde konsultiert wird, oftmals schon ein auf § 11 BDSG gestützter Vertragsentwurf vor. Dies ist – soweit man es „datenschutzpragmatisch" sieht – eher nicht problematisch, weil das Bundesdatenschutzgesetz, was die erforderlichen technischen und organisatorischen Anforderungen an die Datenverarbeitung betrifft, im Vergleich mit dem Hessischen Datenschutzgesetz nicht weniger verlangt (vgl. § 9 BDSG einerseits, § 10 HDSG andererseits).

Dennoch ist es aber datenschutzrechtlich geboten, das Hessische Datenschutzgesetz in einer solchen Situation in die vertraglichen Vereinbarungen zwischen der hessischen öffentlichen Stelle und dem Privatunternehmen zu integrieren. Das verlangt nämlich § 4 Abs. 3 HDSG, u. a. mit der Konsequenz, dass das Privatunternehmen in seiner Funktion als Auftragnehmer nicht mehr (nur) der nach dem Bundesdatenschutzgesetz zuständigen Aufsichtsbehörde unterstellt ist (§ 38 BDSG), sondern (auch) der Kontrolle des Hessischen Datenschutzbeauftragen.

Zu der üblichen gesetzlichen Datenschutzaufsicht nach § 38 BDSG tritt also noch die auf der Grundlage von § 4 Abs. 3 HDSG obligatorisch zu vereinbarende Datenschutzkontrolle des Hessischen Datenschutzbeauftragten hinzu. Die Vorschrift nimmt also Auftragnehmer in die Pflicht, für die ansonsten das HDSG nicht gelten würde, sowie hessische öffentliche Stellen als Auftraggeber.

§ 4 Abs. 3 HDSG

Sofern die Vorschriften auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragen unterwirft. ...

Ist schon § 4 HDSG nichtöffentlichen Stellen, die als Auftragnehmer für (hessische) öffentliche Stellen tätig sein wollen, oft nicht bekannt, so gilt das erst recht für § 80 SGB X, der zu beachten ist, wenn nicht-öffentliche Stellen als digitale Dienstleister personenbezogene Daten im Auftrag für die Sozialverwaltung verarbeiten.

In diesem Bereich gelten dann aber wieder die allgemeinen Aufsichtszuständigkeiten (§ 80 Abs. 6 SGB X). Für den nichtöffentlichen Auftragnehmer ist also nur die Aufsichtsbehörde im Sinne von § 38 BDSG zuständig und nicht zusätzlich der Hessische Datenschutzbeauftragte mit Blick auf § 4 Abs. 3 HDSG. Um es an einem Beispiel zu verdeutlichen: Vor der Zusammenlegung des öffentlichen und des nichtöffentlichen Bereichs in Hessen im Jahr 2011 war im Sozialwesen für einen nichtöffentlichen Auftragnehmer mit Sitz in Hessen das Regierungspräsidium Darmstadt zuständig.

§ 80 SGB X ist bislang in einem Punkt datenschutzrechtlich besonders streng, wird aber mit Blick auf die Datenschutzgrundverordnung (Auftragsverarbeitung, Art. 28) per Gesetzesnovellierung (§ 80 SGB X neu) milder gefasst. Markantester Ausdruck des bisherigen § 80 SGB X ist nämlich das Verbot, dass die öffentliche SGB-Stelle als Auftraggeber den mit einer bestimmten Aufgabenwahrnehmung verbundenen Datenbestand komplett auf den nicht-öffentlichen Auftragnehmer überträgt (§ 80 Abs. 5 SGB X).

§ 80 Abs. 5 SGB X

Die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag durch nicht-öffentliche Stellen ist nur zulässig, wenn

1. ...
2. der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst. Der überwiegende Teil der Speicherung des gesamten Datenbestandes muss beim Auftraggeber verbleiben.

Dahinter steht der (jedenfalls in der heutigen Zeit) nicht mehr überzeugende Gedanke, dass Auftragsdatenverarbeitung durch eine nichtöffentliche Stelle im Sozialbereich eigentlich unterbleiben soll; in Abkehr hiervon ist aber bezeichnenderweise schon bei der Einführung der Grundsicherung für Arbeitsuchende, des SGB II (ugs.: „Hartz IV“), im Jahr 2004 diese Einschränkung bei der Speicherung ausdrücklich aufgehoben worden (§ 51 SGB II).

§ 51 SGB II

Die Träger der Leistungen nach diesem Buch dürfen abweichend von § 80 Abs. 5 des Zehnten Buchs zur Erfüllung ihrer Aufgaben nach diesem Buch einschließlich der Erbringung von Leistungen zur Eingliederung in Arbeit und Bekämpfung von Leistungsmissbrauch nichtöffentliche Stellen mit der Erhebung, Verarbeitung und Nutzung von Sozialdaten beauftragen, auch soweit die Speicherung der Daten den gesamten Datenbestand umfasst.

Anfragende öffentliche und nichtöffentliche Stellen habe ich auf die oben skizzierte Rechtslage hingewiesen.

9. Schulen, Hochschulen

9.1
Personenbezogenen Daten in einem Teilnahmezertifikat eines Fort- oder Weiterbildungsinstituts

Die Nennung personenbezogener Daten in einem Teilnahmezertifikat unterliegt dem Grundsatz der Erforderlichkeit gemäß § 11 Abs. 1 Hessisches Datenschutzgesetz sowie den allgemeinen Geboten der Datenvermeidung und der Datensparsamkeit. Allgemeinverbindliche Regelungen über den Umfang personenbezogener Merkmale in derartigen Dokumenten gibt es nicht.

Der Anlass

Das Institut für Arbeits- und Praxisforschung und Praxisentwicklung (ISAPP) ist als sog. An-Institut der Hochschule RheinMain in Wiesbaden angegliedert. Bei An-Instituten handelt es sich um rechtlich selbstständige Einrichtungen an Hochschulen, die zwar organisatorisch, personell und räumlich mit diesen verflochten, aber kein integraler Bestandteil der Hochschule selbst sind.

Das ISAPP forderte von einer Teilnehmerin für die Ausstellung des Teilnahmezertifikates neben dem Namen das Geburtsdatum und den Geburtsort. Als diese sich weigerte, die Angaben zur Verfügung zu stellen, erhielt sie statt des Zertifikates eine Teilnahmebescheinigung. Das wollte die Teilnehmerin so nicht akzeptieren. Sie wandte sich daher an mich.

Die Rechtsabteilung der Hochschule RheinMain vertrat in Beantwortung meiner Anfrage die Auffassung, dass die Erhebung der Daten rechtmäßig und für die Ausstellung eines Zertifikates erforderlich sei. Da es sich bei einem Zertifikat – im Unterschied zu einer bloßen Teilnahmebescheinigung – um ein „förmliches“ Dokument handele, welches den Teilnehmern individualisierend und „fälschungssicher“ zugeordnet werden müsse, sei die Forderung nach Geburtsdatum und Geburtsort folgerichtig.

Die Hochschule begründete im Weiteren, dass die Verarbeitung der personenbezogenen Daten auf § 11 HDSG gestützt werden könne, da die Daten zur Aufgabenerfüllung und den damit verbundenen Zweck für das Institut erforderlich seien. Die Entwicklung und das Angebot von

Weiterbildungsmaßnahmen gehöre zu den Aufgaben der hessischen Hochschulen und umfasse auch die Ausstellung entsprechender Hochschulzertifikate, wofür es unabdingbar sei, dass eine zweifelsfreie Identifikation der Teilnehmerinnen und Teilnehmer ermöglicht werde. Damit könne man Verwechslungen bei Namensgleichheit ausschließen oder Täuschungsfällen vorbeugen. Schließlich sei die Nennung von Geburtstag und Geburtsort vergleichsweise auch gängige Praxis bei der Ausstellung von Bachelor- und Masterzeugnissen.

Rechtliche Bewertung

Zunächst stellt sich die Frage, ob und worin der Unterschied zwischen einer Teilnahmebescheinigung und einem Zertifikat besteht. Nach einer Definition der Industrie- und Handelskammer Düsseldorf bestätigt die **Teilnahmebescheinigung** die Anwesenheit und ist keine Bescheinigung im Sinne einer Bewertung von Leistungen. Das **Zertifikat** ist danach eine qualifizierte Teilnahmebescheinigung, um z. B. einen bestandenen Test zu bestätigen, setzt eine festgelegte Anwesenheitspflicht voraus und wird ausgestellt auf der Grundlage einer Dokumentation, die jederzeit überprüfbar ist.

Im streitigen Fall wurden die von der IHK genannten Parameter in dem als Zertifikat vorgesehenen Dokument des ISAAP genannt, allerdings dann als Teilnahmebescheinigung ausgestellt. Für das Zertifikat hätte die Betroffene das Geburtsdatum und den Geburtsort nennen müssen. Erscheint schon dies nicht nachvollziehbar zu sein, muss auch die Frage nach der Rechtsgrundlage der Datenerhebung gestellt werden und ob diese zwingend für die Ausstellung eines Zertifikates ist. Bereichsspezifische Normen gibt es keine. Weder im Hochschulrecht ist hierzu etwas festgelegt noch greifen die rechtlichen Vorgaben zur Ausstellung eines Arbeitszeugnisses.

§ 630 BGB

Bei der Beendigung eines dauernden Dienstverhältnisses kann der Verpflichtete von dem anderen Teil ein schriftliches Zeugnis über das Dienstverhältnis und dessen Dauer fordern. Das Zeugnis ist auf Verlangen auf die Leistungen und die Führung im Dienst zu erstrecken. Die Erteilung des Zeugnisses in elektronischer Form ist ausgeschlossen. Wenn der Verpflichtete ein Arbeitnehmer ist, findet § 109 der Gewerbeordnung Anwendung.

§ 109 Abs. 1 GewO

Der Arbeitnehmer hat bei Beendigung des Arbeitsverhältnisses Anspruch auf ein schriftliches Zeugnis. Das Zeugnis muss mindestens Angaben zu Art und Dauer der Tätigkeit (einfaches Zeugnis) enthalten. Der Arbeitnehmer kann verlangen, dass sich die Angaben darüber hinaus auf Leistung und Verhalten im Arbeitsverhältnis (qualifiziertes Zeugnis) erstrecken.

Nach § 630 BGB und nach § 109 GewO besteht für den Arbeitnehmer der Anspruch auf Erteilung eines Zeugnisses. Nach § 109 Abs. 1 GewO muss das Zeugnis schriftlich ausgestellt werden. Die Nennung von Geburtsdatum und Geburtsort sind nicht ausdrücklich genannt, können aber mit Zustimmung der Betroffenen aufgenommen werden.

Der Hinweis auf die Generalnorm des § 11 Abs. 1 HDSG greift ebenfalls nicht.

§ 11 Abs. 1 HDSG

Die Verarbeitung personenbezogener Daten ist ... zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist. Die Erforderlichkeit einer Datenübermittlung muss bei einer der beteiligten Stellen vorliegen.

Erforderlich ist die Verarbeitung, wenn die Verwendung der Daten zur Erreichung des konkreten Zwecks objektiv geeignet und im Verhältnis zum angestrebten Zweck auch notwendig ist. Die Verwaltung muss sich bei der Datenverarbeitung auf das zur rechtmäßigen Aufgabenerfüllung unerlässliche Minimum beschränken (Dembowski in Schild/Ronellenfitsch, Kommentar zum HDSG, zu § 11 Rdnr. 13). Angesprochen sind in diesem Kontext ebenfalls die allgemeinen Gebote von Datensparsamkeit und Datenvermeidung.

Auch der Hinweis, die Datenerhebung diene der zweifelsfreien Identifikation und minimiere eine mögliche Verwechslung oder gar einen Betrug, greift nicht. Um Zweifel an einer Identität zu klären, sind in der Regel Recherchen bei der das Zertifikat (oder die Teilnahmebescheinigung) bestätigenden Einrichtung erforderlich. Ein Abgleich nur der Daten in der Urkunde und z. B. dem Personalausweis ist hier nicht zielführend. Hinzu kommt, dass die Daten einer großen Mehrheit erhoben werden, um einer faktisch kleinen Klientel auf die Spur zu kommen. Hier scheint auch das Prinzip der Verhältnismäßigkeit nicht berücksichtigt zu sein.

Im vorliegenden Fall kam hinzu, dass die personenbezogenen Daten im Nachgang, explizit zur Ausstellung des Zertifikates, eingefordert wurden. Nach meinem Schriftwechsel mit der Hochschule hat das angegliederte Institut das Online-Anmeldeverfahren geändert und die zusätzlichen „Pflichtfelder“ Geburtsdatum und Geburtsort in das Formular aufgenommen.

Weiteres Verfahren

Ich habe der Hochschule die Gelegenheit zur nochmaligen Stellungnahme eingeräumt. Zudem habe ich den Streitfall im Arbeitskreis der Datenschutzbeauftragten zur Diskussion gestellt. Meine Position wurde dort kritisch zur Kenntnis genommen. Ich selbst werde mich im Kontakt mit dem Ministerium für Wissenschaft und Kunst darum bemühen, eine Aufnahme verbindlicher Erhebungsnormen für diese Fallkonstellationen in das Hessische Hochschulgesetz einzubringen.

9.2
Schultagebuch für Kinder beruflich Reisender in digitaler Form

Seit einigen Jahren berate ich eine Arbeitsgruppe der Kultusministerkonferenz (KMK), die sich mit der Digitalisierung der Prozesse rund um das Lernen von Kindern beruflich Reisender befasst. Dabei geht es insbesondere um die Schaffung eines elektronischen Schultagebuchs sowie einer Kommunikations- und Informationsplattform insbesondere für die sog. Bereichslehrkräfte. Dies sind jene Lehrer, die sich für die Zeit des Aufenthaltes der Kinder an einem bestimmten Ort in Deutschland um die schulische Betreuung kümmern. Die datenschutzrechtlichen Anforderungen hierfür habe ich in einem Papier formuliert.

9.2.1
Wer sind Kinder beruflich Reisender?

Die Kinder beruflich Reisender sind eine Schülergruppe, deren Bildungsweg durch einen häufigen Schulwechsel oft über die Ländergrenzen in Deutschland und teilweise auch über Deutschland hinaus bestimmt ist. Kinder beruflich Reisender sind vor allem Kinder aus Schaustellerfamilien, von Zirkusangehörigen, von ambulanten Händlern, Puppenspielern und anderen Berufsgruppen. Die Reisetätigkeit führt zur Verkürzung der Unterrichtszeiten, wodurch

eine ausreichende Begleitung der schulischen Laufbahn dieser Kinder und Jugendlichen, angefangen von der vorschulischen Betreuung bis hin zur beruflichen Bildung, vielfach erschwert wird.

Vor diesem Hintergrund gibt es – in Abstimmung mit Verbänden und Elternvertretern dieser Berufsgruppen – vielfältige Bemühungen der Länder, die Lernbedingungen dieser Kinder zu verbessern und ihnen einen Schulabschluss zu ermöglichen. Ein wichtiger Schritt hierbei war der 2003 gefasste Beschluss der Kultusministerkonferenz, den Lernweg und den Lernstand der Kinder in einem Schultagebuch zu dokumentieren und somit an den ständig wechselnden Lernorten den jeweiligen Lehrkräften gezielten Unterricht zu ermöglichen. Weitere Angebote für Kinder beruflich Reisender, wie z. B. das System von Stamm- und Stützpunktschulen, die Unterstützung durch Bereichslehrkräfte, die in 14 Ländern eingesetzt werden, Fernlern- und E-Learning-Angebote, das Arbeiten mit individuellen Lernplänen etc. sind in Handreichungen zum Schultagebuch, die auf den jeweiligen Länderseiten abrufbar sind, näher beschrieben.

9.2.2
Digitalisierung soll Zusammenarbeit aller Beteiligten an der Betreuung der Kinder beruflich Reisender optimieren

Das Schultagebuch wird von der sogenannten Stammschule (Schule am melderechtlichen Wohnsitz der Eltern) der Schülerin oder dem Schüler übergeben und begleitet diese über die Schullaufbahn. Es enthält Informationen und Hinweise zum Lernprozess des reisenden Kindes oder Jugendlichen. Jedes Schultagebuch enthält von der Stammschule erstellte, individuelle Lernpläne für die Fächer Deutsch, Mathematik und Fremdsprache. In ihm werden die behandelten Inhalte und die Schulbesuchstage dokumentiert. Seine Verwendung ist in allen Ländern verpflichtend.

Das Buch wird bislang in Papier geführt und von den jeweiligen Stützpunktschulen oder Bereichslehrkräften befüllt. Problematisch wird es, wenn das Schultagebuch verloren geht. Auch sind Informationen, die von der Stammschule an die Stützpunktschule gehen sollen und umgekehrt, nicht immer auf einem aktuellen Stand. Um derartige Probleme künftig auszuschalten, wird die Digitalisierung des Schultagebuchs in Form einer (cloudbasierten) IT-Plattform (Digitales Lernen unterwegs – DigLu) angestrebt, die allen Beteiligten der Betreuung der Kinder beruflich Reisender zur Kommunikation und Information zur Verfügung steht. Als zentrales Informationssystem soll das DigLu dem länderübergreifenden Informationsaustausch zwischen Bereichslehrern, Stammschulen, Stützpunktschulen, der Schulaufsicht und anderen

Einrichtungen dienen, die temporär für die schulische Betreuung (Bildung und Erziehung) von Kindern beruflich Reisender zuständig sind. Das DigLu soll den gesamten Betreuungsrahmen mit einem Bezug zum jeweiligen Land und in seiner Orientierung an den Stammschulen der Kinder beruflich Reisender flankieren. Zudem soll es eine einfache und schnelle Kommunikation zwischen den beteiligten Personen und Institutionen ermöglichen.

Zum Beispiel erstellt die Stammschule für die Reisezeiten der Kinder einen individuellen Lernplan. Dieser ist Grundlage für den Unterricht bzw. den Lernweg der Kinder. Die Dokumentation des Lernwegs der Kinder erfolgt während der Reisezeiten über das Portfolio. Lernplan und Portfolio werden in das DigLu eingebunden.

Das DigLu soll somit folgende Grundfunktionen erfüllen:
– Bereitstellung einer Kommunikationsplattform für die beteiligten Lehrkräfte,
– Bereitstellung personenbezogener Stammdaten der reisenden Schülerinnen und Schüler und deren Erziehungsberechtigten,
– Bearbeitung und Weitergabe individueller Lerndaten (digitales Portfolio),
– Bearbeitung und Weitergabe individueller Lernpläne (digitales Schultagebuch).

9.2.3
Datenschutzrechtliche Anforderungen an ein Informationssystem

Gegenüber der KMK-Arbeitsgruppe habe ich datenschutzrechtliche Anforderungen formuliert, deren Einhaltung im Rahmen der Nutzung einer (cloudbasierten) Anwendung gewährleistet sein muss:

a) Technische Vorgaben für ein datenschutzkonformes System

In Frage kommen ein servergestütztes System oder eine webbasierte Cloud-Lösung. Rechtlich nicht zwingend, jedoch aus Gründen der Kontrollmöglichkeiten sowie der Akzeptanz zielführend ist eine technische Lösung in Deutschland oder einem anderen Land der Europäischen Union mit einem hohen Datenschutzniveau (z. B. Österreich, Niederlande etc.).

b) Schutzbedarf der Daten

Hier kommt es maßgeblich darauf an, welche Art von personenbezogenen Daten eingespeist werden. In der Regel ist von einem normalen Schutzbedarf auszugehen. Dies könnte sich jedoch dann ändern, sollten z. B. Daten zu den Familienverhältnissen, Gesundheitsdaten (Förderbedarf) o. Ä. eingespeichert werden. Mit Blick auf Artikel 9 der DS-GVO (Verarbeitung

besonderer Kategorien personenbezogener Daten) muss dann geprüft werden, ob zusätzliche Sicherheitsmaßnahmen durch den Plattformbetreiber und die eingebundenen Stellen zu ergreifen sind.

c) Datenübermittlung

Die Übermittlung der personenbezogenen Daten erfolgt über das Internet. Um den Schutz hierbei zu gewährleisten, ist eine dem aktuellen technischen Stand Rechnung tragende Ende-zu-Ende-Verschlüsselung beim Datentransport erforderlich.

d) Datenabrufe und Datenspeicherung

Um eine nicht autorisierte Speicherung der personenbezogenen Daten auf einem dienstlichen oder privaten Rechner, z. B. einer Bereichslehrkraft, zu verhindern, ist eine Terminalserver-Lösung anzustreben. Damit ist es möglich, die Daten unabhängig vom Endgerät zur Verfügung zu stellen. Dabei verlassen die Daten nicht das interne Netzwerk, sondern lediglich die Bildschirmausgabe wird zum Terminal übertragen. Die Speicherung von Daten bleibt davon unberührt. Bei Ausfall, Diebstahl oder Virenbefall des lokalen Endgeräts (Client) werden die im geschützten Server (oder der Cloud) gespeicherten Daten weder kompromittiert noch gehen sie verloren.

e) Zugriffssschutz

Hier sollte eine Zwei-Faktor-Authentifizierung (2FA) angestrebt werden. Diese dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und inbesondere unabhängiger Komponenten (Faktoren). Die Faktoren können sein:

– etwas, das der Nutzer besitzt wie z. B. ein Hardeware-Token,
– etwas, das der Nutzer weiß, z. B. eine PIN oder eine TAN,
– etwas, das als körperliches Charakteristka untrennbar zum Nutzer gehört, wie z. B. ein Fingerabdruck o. a.

f) Rollen- und Berechtigungskonzept

Ein server- oder plattformgestütztes System muss zwingend die Implementierung eines dezidierten Rollen- und Berechtigungskonzepts ermöglichen.

g) Stammschule

Die Stammschule ist rechtlich i. S. d. Datenschutzgesetze der Länder als Daten verarbeitende Stelle und damit auch als verantwortliche Stelle anzusehen. Ein Berechtigungskonzept

beschreibt ein System, das die Struktur und die Verfahren für Zugriffsrechte und die Zugriffskontrolle festlegt.

Für die Vergabe von Berechtigungen muss zunächst innerhalb der Stammschule gesorgt werden. Nur ein bestimmter Personenkreis darf den Zugriff auf das System erhalten. Dabei sind mögliche Rollen und Berechtigungen für jeden Nutzer vorab zu definieren:

– Lesen von Daten,
– Schreiben von Inhalten in das System,
– Verändern von Daten im System,
– Löschen von Daten (soweit keine automatisierte Löschprozesse implementiert sind).

h) Stützpunktschule

Die Stützpunktschule ist temporär der Lernort für die Schüler. Die Stützpunktschule muss Lehrer benennen, welche die schulischen Leistungen in einem BIS dokumentieren. Dabei muss sichergestellt werden, dass die Berechtigungen dieser Lehrer nicht jenen der zuständigen Lehrkräfte in der Stammschule entsprechen.

Beispiel: es ist grundsätzlich nicht erforderlich, Lehrkräften einer Stützpunktschule oder Bereichslehrkräften eine Löschberechtigung einzuräumen. Bereits die Möglichkeit, Daten nach deren Einstellung in ein Informationssystem noch verändern zu können, ist restriktiv zu behandeln.

i) Bereichslehrkräfte

Die Bereichslehrkräfte benötigen ebenfalls einen temporären Zugriff, um Kommunikation mit den Schülern zu betreiben, Aufgaben zu stellen und Bewertungen oder andere Informationen für die Stammschule in ein Informationssystem einstellen zu können.

j) Administration der Zugriffsberechtigungen

Ausgesuchte Lehrkräfte der Stammschule müssen die internen und externen Zugriffe festlegen. Hierzu bedarf es einer Anwendung, die möglichst nutzerfreundlich konfiguriert ist, d. h. der Aufwand hierfür überschaubar bleibt und sich die Komplexität der Anwendung hierfür in Grenzen hält. Wichtig erscheint zudem ein Verfahren, welches die zweifelsfreie Feststellung der Identität einer externen Lehrkraft im Rahmen der Rechtevergabe ermöglicht.

Eine zeitnahe Entziehung der Berechtigungen dann, wenn der Schüler die Stützpunktschule verlässt oder die Bereichslehrkraft nicht mehr zuständig ist, muss gewährleistet sein. Zumindest ist zu überlegen, von vorneherein eine zeitliche Begrenzung der Berechtigungen zu generieren, die dann im erforderlichen Fall verlängert werden könnten.

Je nach Erfordernis (Schutzbedarf der Daten) ist zu überlegen, ob der Einsatz eines VPN (Virtual Private Network) erforderlich sein könnte.

k) Protokollierung

Systemseitig muss eine hinreichende Protokollierung der Nutzeraktivitäten gegeben sein. Bei der Nutzung des Informationssystems im Rahmen einer Lernplattform ist zu prüfen, ob die Auswertung sog. Nutzungsdaten der Schüler (z. B. LOGIN, Dauer der Verweilzeit auf der Plattform, Zeitpunkt der Nutzung der Plattform, IP-Adresse) oder die von pädagogischen Prozessdaten (z. B. Testergebnisse, Anzeige der benötigten Zeit für die Lösung einer Aufgabe durch den Schüler) durch die berechtigten Lehrkräfte möglich sein soll. Diese Art von „Profiling“ ist entsprechend den Vorgaben der DS-GVO dem Nutzer, also den Schülern bzw. den Erziehungsberechtigten, mitzuteilen. Tracking-Daten werden grundsätzlich für Learning Analytics Zwecke genutzt. Im vorliegenden Fall ist zu prüfen, ob derartige Funktionalitäten in einer ersten Ausbaustufe erforderlich sind. Ggf. müssten in weiteren Schritten die rechtlichen Aspekte hierzu, wie sie sich aus der DS-GVO und den landesspezifischen Datenschutzgesetzen ergeben, beleuchtet werden. Hinsichtlich der Speicherdauer ist zunächst von einem Zeitraum von 90 Tagen auszugehen.

l) Mobiles Device-Management

Eine wesentliche datenschutzrechtliche Fragestellung betrifft die Endgeräte, welche durch die Lehrkräfte (unabhängig davon, ob diese der Stamm- oder der Stützpunktschule angehören) genutzt werden. Hier bedarf es zunächst der Klärung, ob Lehrkräfte ausschließlich dienstliche Geräte nutzen, welche durch die Schule (oder den Dienstleister) vorkonfiguriert sind und bestimmte, vorgegebene (Schutz-)Standards einhalten.

Beim Einsatz privater Endgeräte ergibt sich die Problematik der privaten und dienstlichen Nutzung auf einem (privaten) Gerät. Daraus leiten sich bestimmte Anforderungen an die Datensicherheit ab (Stichwort: Häuslicher Arbeitsplatz der Lehrkraft). So wäre in einem solchen Fall durch technische oder organisatorische Maßnahmen sicherzustellen, dass keine dienstlichen Daten auf einem privaten Endgerät gespeichert werden (können). Auch sollte ein Transport von personenbezogenen Daten (z. B. USB-Sticks) ausgeschlossen werden, da systemseitig ein derartiges Erfordernis nicht besteht.

m) Systemseitige Standards

Festzulegen ist, welche technischen und organisatorischen Anforderungen ein Informationssystem dem jeweiligen Nutzer im Rahmen des Zugangs zum System abfordert. So wären beispielsweise folgende Parameter zwingend vorzuschreiben:

– Verwendung eines bestimmten, aktuellen Browser,
– Einsatz eines leistungsfähigen Virenscanner,
– Verwendung eines bestimmten Betriebssystems.

Mit diesen Vorgaben wird erreicht, dass die zu nutzenden Endgeräte bestimmten, festgelegten technischen Standars entsprechen und auch auf dieser Ebene ein Informationssystem vor einer möglichen Kompromittierung geschützt wird.

n) Technischer Support

Durch den Dienstleister, der ein Informationssystem entwickelt, ist ein technischer Support sicherzustellen, der den Ansprüchen u. a. hinsichtlich der Verfügbarkeit der personenbezogenen Daten Rechnung trägt. Die Anwender müssen zu jedem Zeitpunkt die Möglichkeit erhalten, ggf. vorhandene technische Probleme im Rahmen der Anwendung durch den Kontakt mit dem Dienstleister einer Lösung zuzuführen.

o) Mögliche Auswirkungen der DS-GVO auf die Anwendung

Ob und ggf. welche Auswirkungen die DS-GVO auf ein BIS haben könnte, bedarf einer näheren Betrachtung. Je nach Sensitivität der Daten wäre z. B. eine Datenschutzfolgenabschätzung i. S. v. § 35 DS-GVO erforderlich. Weitere Parameter können Informationsrechte der Betroffenen (Schüler, Eltern und Lehrkräfte) oder Löschungspflichten der Daten verarbeitenden Stellen, also der Stammschulen, sein.

9.2.4
Schlussbetrachtung und Zusammenfassung

Gegen die Einführung des DigLu bestehen keine datenschutzrechtlichen Einwände, soweit die erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz und der Datensicherheit umgesetzt werden. Die Anforderungen an ein Informationssystem sind hinsichtlich des Datenschutzes anspruchsvoll, jedoch realisierbar. Verwiesen sei in diesem Zusammenhang auf eine von meinem Haus geprüfte Cloud-Anwendung, welche von diversen Frankfurter Beratungs- und Förderzentren (BFZ) genutzt wird und für bestimmte Anforde-

rungen zumindest die Möglichkeit einer Nutzungsalternative bieten könnte (vgl. hier auch meinen 45. Tätigkeitsbericht, Ziff. 3.4.3: Modernes Bildungsmanagement in der Schule).

Folgende datenschutzrechtliche Anforderungen muss ein Informationssystem erfüllen, die sich am Schutzbedarf der personenbezogenen Daten auszurichten haben:

- Ende-zu-Ende-Verschlüsselung im Rahmen der Datenübertragung,
- Terminalserverlösung,
- Zwei-Faktor-Authentifizierung,
- Verschlüsselung der auf einem Server oder in einer Cloud abgelegten Daten,
- Rollen und Berechtigungskonzept
  - für die Lehrkräfte der Stammschule,
  - für die Lehrkräfte der Stützpunktschule,
  - für die Bereichslehrkräfte,
- Administrationsberechtigungen für ausgewählte Kräfte der Stammschule,
- angemessene Protokollierung der Systemaktivitäten,
- hinreichend technischer Support im Zusammenhang mit der Verfügbarkeit der personenbezogenen Daten.

Bei der Neuentwicklung eines Informationssystems erscheint es zweckmäßig, von Anfang an hohe Standards im Hinblick auf Datenschutz und Datensicherheit anzustreben. Zum Einen gebietet dies insbesondere die Datenschutz-Grundverordnung, die am 25.05.2018 in Kraft tritt. Aber auch die 16 Landesdatenschutzgesetze machen diese Standards erforderlich (s. a. technische und organisatorische Maßnahmen zum Datenschutz und der Datensicherheit, so z. B. § 10 Abs. 2 HDSG, § 10 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen, § 9 Abs. 3 Landesdatenschutzgesetz Baden-Württemberg).

Da es sich hier zudem um eine bundesweite, automatisierte Datenverarbeitung handelt, erscheint es zweckmäßig und aus Gründen der Akzeptanz zwingend zu sein, ein Produkt entwickeln zu lassen oder zu beschaffen, welches die maßgeblichen Kriterien ohne jedwede Einschränkung erfüllt. Ob nun Neuentwicklung (die sich zeitintensiv gestalten könnte) oder die Nutzung eines ggf. bereits auf dem Markt befindlichen Produkts: Die Auftraggeber müssen in enger Absprache mit einem potentiellen Partner nicht nur die inhaltlichen, sondern in gleichem Maße auch die technisch-organisatorischen Fragestellungen von Anfang an intensiv begleiten und die entsprechenden Parameter hierzu setzen.

9.2.5
Ausblick

Die Arbeitsgruppe der KMK hat im September vergangenen Jahres ein Software-Unternehmen, welches die Anwendung DiLer (Digitales Lernen) betreibt, beauftragt, auf der Grundlage von DiLer eine Plattform zu entwickeln, welche den inhaltlichen und datenschutzrechtlichen Vorgaben entspricht. Zudem wurde das Projekt im Unterarbeitskreis Datenschutz und Schulen der Datenschutzbeauftragten von Bund und Ländern vorgestellt. Mit der frühzeitigen Einbindung der Aufsichtsbehörden für den Datenschutz soll von Beginn an dieses Digitalisierungsprojekt im Bildungsbereich gut aufgestellt sein.

9.3
Datenschutzkonformer Einsatz von Microsoft Office 365 an Schulen

Der Einsatz von Microsoft Office 365 in der sog. „Deutschland-Cloud“ durch hessische Schulen stößt auf keine grundsätzlichen datenschutzrechtlichen Bedenken. Die Nutzung muss sich jedoch zunächst auf den pädagogischen Bereich beschränken. Zudem müssen die Schulen jene Werkzeuge, welche Microsoft zur Umsetzung von Datenschutz und der Datensicherheit in der Cloud zur Verfügung stellt, sinnvoll und sachgerecht einsetzen.

Eine jahrelange Diskussion führt zu keinem Ergebnis

Seit Jahren erhalte ich regelmäßig Anfragen von Schulen, ob die Nutzung der Office 365-Cloud möglich sei. Ebenso seit Jahren beschäftigen sich die Aufsichtsbehörden von Bund und Ländern in verschiedenen Arbeitskreisen mit diesem Thema.

Vorbehalte wurden stets dahingehend geäußert, dass die europäische Cloud von Microsoft mit Rechenzentren in Dublin und Amsterdam nicht sicher vor einem möglichen Zugriff u. a. US-amerikanischer Geheimdienste sei und deutsche, öffentliche Stellen und damit auch die Schulen nicht die Sicherheit der Datenverarbeitung, im vorliegenden Fall von Schüler- und Lehrerdaten, gewährleisten könnten. Microsoft versicherte zwar immer wieder, bislang keine Daten europäischer Kunden auf Anordnung von US-Gerichten oder Anfragen von US-behörden herausgegeben zu haben. Dennoch blieb das Misstrauen der Aufsichtsbehörden groß.

Kultusministerium zeigt Interesse

Im Sommer 2015 folgte ich einer Einladung des Hessischen Kultusministeriums, um zusammen mit Vertreten von Microsoft auszuloten, ob und unter welchen Bedingungen ein datenschutzkonformer Einsatz der Cloud im Schulbereich möglich sein könnte. Es zeigte sich damals, dass eine Fülle klärungsbedürftiger Fragen von Microsoft nicht zufriedenstellend beantwortet werden konnten, was einer baldigen Lösung im Wege stand. Für das Kultusministerium von Interesse erschien die Möglichkeit, über die Cloud den 70.000 Lehrkräften in Hessen eine einheitliche, dienstliche E-Mail-Adresse anbieten zu können.

Microsoft Deutschland Cloud eröffnet neue Perspektiven

Anfang 2016 ging Microsoft mit der sog. „Deutschland-Cloud“ an die Öffentlichkeit. Der Konzern hatte eine Infrastruktur aufgebaut, welche es ermöglicht, die Verarbeitung auch personenbezogener Daten in Deutschland vorzunehmen. Hierzu wurden zwei Rechenzentren in Frankfurt am Main und Magdeburg geschaffen, in denen die Daten gespeichert sind. Zudem hat Microsoft mit der T-Systems International GmbH mit Sitz in Frankfurt am Main einen sog. „Datentreuhänder“ beauftragt. Dieser dient als „Torwächter“, der Zugriffe von Microsoft im Wege des Supports oder der Software- bzw. Hardware-Installation begleitet, kontrolliert und ggfs. beendet. Diese begleiteten Zugriffe auf Kundendaten werden über zwei sog. Cloud-Control-Center organisiert, die in Berlin und Magdeburg angesiedelt sind. Diese werden von Mitarbeitern der T-Systems gesteuert. Von dort erfolgt auch die Freischaltung der Zugriffe für Microsoft.

Die Cloud-Dienste Azure und Office 365 entsprechen dem Standard von ISO/IEC 27018, welcher einem „Code of practice“ entspricht. Zudem ist eine ISO 27001-Zertifizierung auf der Basis für IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik erfolgt.

Rechtliche Bewertung

Die Verarbeitung personenbezogener Daten in der Microsoft „Deutschland-Cloud“ lässt sich im Rahmen des § 83 Abs. 1 des Hessischen Schulgesetzes (HSchG) in Verbindung mit § 1 Abs. 1 der Verordnung über die Verarbeitung personenbezogener Daten an Schulen datenschutzkonform gestalten. Danach dürfen personenbezogene Daten von Schülern, deren Eltern und Lehrkräften verarbeitet werden, soweit dies zur rechtmäßigen Erfüllung des Bildungs-

und Erziehungsauftrages und für einen jeweils damit verbundenen Zweck erforderlich ist. Insoweit habe ich keine rechtlichen Vorbehalte gegen die geschilderte Art der Verarbeitung personenbezogener, schulischer Daten aus dem pädagogischen Bereich der Schulen.

Ohnehin sehen weder das Hessische Datenschutzgesetz noch das Bundesdatenschutzgesetz ein Verbot der Übermittlung personenbezogener Daten in Drittstaaten vor.

Wesentliche Aspekte einer technischen Umsetzung

Zur Beantwortung der Frage, ob durch Schulen als Daten verarbeitende Stellen ein datenschutzgerechter Betrieb des Verfahrens gewährleistet werden kann, wurden im Wesentlichen drei Bereiche näher betrachtet. Dabei wurden die Maßstäbe, die sich für pädagogische Plattformen entwickelt haben, für die Bewertung zu Grunde gelegt.

Sollten Schulen darüber hinaus anstreben, Daten mit weitergehendem Schutzbedarf auf der Basis der Microsoft „Deutschland-Cloud“ zu verarbeiten, müsste deshalb eine gesonderte Betrachtung erfolgen. Nachfolgende Fragestellungen galt es zu untersuchen:

1. Ist das von Microsoft konzipierte Treuhändermodell technisch geeignet, die Bedenken zu möglichen Zugriffersuchen ausländischer staatlicher Stellen auszuschließen?

   Unter Berücksichtigung der vertraglichen Beziehungen zwischen den Auftraggebern (also den Schulen) und dem Auftragnehmer können technisch und inhaltlich eng begrenzte Zugriffe von Microsoft auf Kundendaten nur in plausiblen Zusammenhängen erfolgen, wenn der Treuhänder den Service-Prozess in allen Phasen aktiv begleitet.

2. Können durch die Microsoft Rechenzentren und die Schulen als verantwortliche Auftraggeber die Empfehlungen zu erforderlichen technischen und organisatorischen Maßnahmen der Orientierungshilfe Cloud-Computing (Ziff. 4 sowie Homepage www.datenschutz.hessen.de) umgesetzt werden?

In einer Reihe von Veranstaltungen und Gesprächen hat Microsoft die grundsätzliche Organisation und Infrastruktur seiner Rechenzentren und die Besonderheiten der „Deutschland Cloud“ erläutert. Dabei wurde deutlich, dass die Rechenzentren für die Wahrung der allgemeinen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität die organisatorisch notwendigen Voraussetzungen bieten. Dazu kann Microsoft auf eine Reihe von Zertifizierungen nach

Ziff. 4.3 der Orientierungshilfe verweisen.
Eine datenschutzgerechte Nutzung der Cloud-Anwendung erfordert aber von den Schulen, dass diese die für alle weiteren Fragen erforderlichen Konzepte entwickeln.

3. Welche konzeptionellen Schritte und Umsetzungen müssen durch Schulen ggf. mit Unterstützung der Schulträger erfolgen, damit das Verfahren allen datenschutzrechtlichen Anforderungen genügt?

   Schulen müssen sich ggf. in Abstimmung mit dem Schulträger zunächst dafür entscheiden, welche Art der Anbindung sie wählen. Microsoft bietet dazu verschiedene Möglichkeiten, die bis zur Kopplung der Verzeichnisdienste des Active Directory (AD) reichen. Unabhängig von der gewählten Variante muss neben der Sicherheit des Verfahrens auch die Integrität der schulischen Netze gewahrt bleiben.

   Damit eng verbunden ist die Erstellung eines Rollen- und Berechtigungskonzeptes, das je nach Nutzung der Anwendung und Art der Anbindung zwischen administrativen Rollen, allgemeinen Lehrkräften, Schülern und ggfs. weiteren Rollen mit besonderen Aufgabenstellungen unterscheiden muss.

   Um neben allgemeinen Verfahrensanforderungen insbesondere jenen der Orientierungshilfe Cloud-Computing zu entsprechen, sind zu den genannten Schritten alle Aspekte der Verfahrensprotokollierung und -dokumentation in einem ergänzenden Konzept zusammenzufassen.

   Da gerade in Cloud-Anwendungen nicht immer einfach sicher zu stellen ist, den Ansprüchen an eine fristgerechte Löschung gerecht zu werden, müssen unter Berücksichtigung der verschiedenen Möglichkeiten des Systems für alle anfallenden, personenbezogenen Daten die notwendigen Löschkonzepte erstellt werden.

Auf der Basis meiner grundsätzlichen Einschätzung zum Einsatz von Office 365 in der Microsoft „Deutschland-Cloud“ haben einzelne Schulen und Schulträger mit Vorüberlegungen und der Erstellung notwendiger Konzepte begonnen. Da sich hieraus eine Reihe von abzustimmenden Detailfragen ergibt, werden meine Mitarbeiter exemplarisch einige Entwicklungen begleiten.

Zusammenfassung

Die Nutzung von Office 365 in der „Deutschland-Cloud“ durch hessische Schulen lässt sich datenschutzkonform umsetzen.

Folgende Punkte sind dabei von besonderer Bedeutung:

– Die Schulen müssen eine datenschutzkonforme Systemarchitektur implementieren, welche Microsoft zwar teilweise zur Verfügung stellt, deren Umsetzung jedoch in der Verantwortung der Schule in Zusammenarbeit mit dem Schulträger liegt und zusätzliche technische und organisatorische Maßnahmen erfordert.
– Jede Schule hat – von besonderen Ausnahmefällen abgesehen – den technischen Support über den Datentreuhänder abzuwickeln. So wird sichergestellt, dass der Datentreuhänder jede Supportanfrage, welche den Zugang zur Plattform oder den Zugriff auf personenbezogene Daten der Schule ermöglicht, überwachen, beenden und protokollieren kann.
– Die Einschaltung bzw. Beteiligung des schulischen Datenschutzbeauftragten sowie des behördlichen Datenschutzbeauftragten des Schulträgers bei der Umsetzung von Maßnahmen ist gem. § 7 Abs. 4 HDSG zwingend erforderlich. Dies muss schriftlich dokumentiert werden.
– Die ab 25.05.2018 wirkende Datenschutz-Grundverordnung (DS-GVO) kann zu weiteren Anforderungen wie möglicherweise einer Datenschutz-Folgenabschätzung führen.
– Nach Ablauf eines Schuljahres muss der Einsatz der Anwendung hinsichtlich der inhaltlichen und datenschutzrechtlichen Parameter evaluiert werden. Soweit erforderlich, müssen Ergänzungen oder Korrekturen vorgenommen werden.

9.4
Unzulässige Datenübermittlung eines Studierendenwerks

Immer wieder kommt es vor, dass öffentliche Stellen an Betroffenen vorbei ohne Rechtsgrundlage oder deren Einwilligung personenbezogene Daten an Dritte übermitteln.

Der Anlass

Eine Studentin hatte über ein Studierendenwerk eine Förderung nach dem Bundesausbildungsförderungsgesetz (BAföG) beantragt und gewährt bekommen. Wenig später erhielt die

Betroffene ein Stipendium der Stiftung der deutschen Wirtschaft, welches sie gegenüber dem Studierendenwerk ordnungsgemäß anzeigte. Die BAföG-Leistungen wurden vom Studierendenwerk nun zurückgefordert, da das Stipendium rückwirkend gewährt wurde und mit dem Zeitraum der BAföG-Gewährung identisch war. Dabei handelte es sich um einen Betrag von 245 Euro.

Gegen den Rückzahlungsbescheid hatten die Studentin bzw. deren Vater, an den die Studentin die Forderung abgetreten hatte, Rechtsmittel eingelegt. Gleichwohl wandte sich das Studierendenwerk an den Stipendiengeber und bat um Verrechnung des Betrages mit den Stipendienleistungen. Gegen diese Vorgehensweise beschwerte sich der Vater der Studentin und Schuldner.

Das Studierendenwerk hielt seine Vorgehensweise durch die Rechtsnorm des § 2 Abs. 6 Nr. 2 BAföG sowie die Verwaltungsvorschrift hierzu gedeckt.

§ 2 Abs. 6 Nr. 2 BAföG

Ausbildungsförderung wird nicht geleistet, wenn der Auszubildende
...
2. Leistungen von den Begabtenförderungswerken erhält.

Entsprechend der Verwaltungsvorschrift zu § 2 zählt die Stiftung der deutschen Wirtschaft zu den Begabtenförderungswerken. Diese Norm enthält keine Rechtsgrundlage für die besagte Datenübermittlung des Studierendenwerks an die Stiftung. Zusätzlich argumentierte man, dass für die Betroffene kein Schaden entstanden und die Daten ja nicht sensitiv seien.

Rechtliche Bewertung

Die Rechtsauffassung des Studierendenwerks ist unzutreffend. Zunächst ist festzustellen, dass in § 2 Abs. 6 Nr. 2 BAföG und der nachgeschalteten Verwaltungsvorschrift nur zum Ausdruck gebracht wird, dass eine „Doppelförderung“ nicht möglich ist. Von einer Befugnisnorm für eine Datenübermittlung kann daher keine Rede sein. Die Studentin hatte sich vielmehr korrekt verhalten und das Stipendium angezeigt. Strittig war in der Folge nicht die Rückzahlung selbst, sondern deren Höhe sowie die Modalitäten hierfür. Zum Zeitpunkt der Anfrage durch

das Studierendenwerk beim Stipendiengeber war das streitige Verfahren noch nicht abgeschlossen, die Möglichkeiten zur Begleichung der Forderung durch das Studierendenwerk noch nicht ausgeschöpft.

Zudem musste ich attestieren, dass das Studierendenwerk personenbezogene Daten ohne Rechtsgrundlage übermittelt hatte.
Das Studierendenwerk hat mir im Nachgang zu seiner Stellungnahme versichert, sich künftig in ähnlich gelagerten Fällen anders zu positionieren und von derartigen Anfragen abzusehen.

9.5
Hessische Schulträger werden über Videoüberwachung an Schulen informiert

Die wichtigsten Fragen zum datenschutzkonformen Einsatz von Videoüberwachung an hessischen Schulen konnten auf einer von mir durchgeführten Informationsveranstaltung für hessische Schulträger geklärt werden.

Wiederholt war das Thema Videoüberwachung an Schulen Bestandteil meiner Tätigkeitsberichte (44. Tätigkeitsbericht, Ziff. 3.4.4; 42. Tätigkeitsbericht, Ziff. 3.3.5.2; 41. Tätigkeitsbericht, Ziff. 3.3.3.3). Anlass, mich mit dieser Thematik erneut zu beschäftigen, war die Beantwortung der entsprechenden Kleinen Anfrage der CDU durch die Landesregierung (LTDrucks. 19/4391).

Durch die vom Kultusministerium beantwortete Frage, in welchen der kreisfreien Städte und Landkreise in Hessen eine Videoüberwachung an Schulen erfolge, wurde mir bekannt, dass lediglich die Städte Darmstadt und Marburg sowie der Landkreis Waldeck-Frankenberg von der Videoüberwachung keinen Gebrauch machen. Alle übrigen Schulträger setzen Videoüberwachung ein. In der Vergangenheit bin ich auch von Schulträgern oder einzelnen Schulen immer wieder zu diesem Thema befragt worden. In einigen Fällen begab ich mich vor Ort und gab Hinweise, ob die Voraussetzungen für eine Videoüberwachung vorlagen und wenn ja, wie diese gesetzeskonform umzusetzen seien. Jedoch waren meine Mitarbeiter und ich uns darüber im Klaren, dass es eine Reihe von Schulträgern bzw. Schulen geben müsse, die von sich aus bereits Fakten geschaffen haben und Videoüberwachung nutzen, ohne dass es einen Kontakt zum HDSB gegeben hätte. Zwar besteht keine Meldepflicht der Schulträger oder der Schulen beim Einsatz derartiger Mittel. In Anbetracht der Bedeutung der Maßnahme, insbesondere des Eingriffs in die informationelle Selbstbestimmung der betroffenen Schülerinnen

und Schüler oder auch der Lehrkräfte habe ich aber stets dafür geworben, meine Beratungskompetenz zu nutzen.

Ich hielt es deshalb für angezeigt, die hessischen Schulträger zu einer Informationsveranstaltung einzuladen, um meine rechtliche Position zu verdeutlichen und Hilfestellung bei Fragen zu geben, wann die Voraussetzungen für eine Videoüberwachung vorliegen können.

Zusammenkunft mit Schulträgern klärte manche Frage

Meine Einladung an die Schulträger stieß auf ein nachhaltiges und positives Echo. Von 32 Schulträgern waren 31 nach Wiesbaden gekommen, um meine Positionen zu dem Thema zu hören und Fragen zu stellen. Auch Vertreter des Kultusministeriums waren zugegen. Meine Mitarbeiter erläuterten die rechtlichen Grundlagen für eine Videoüberwachung, die erforderlichen tatsächlichen Voraussetzungen sowie die Möglichkeiten einer gesetzeskonformen Umsetzung. Im Verlauf der anschließenden Diskussion, in der eine Vielzahl – auch kritischer – Beiträge der Teilnehmer erfolgte, konnten zahlreiche Einzelfragen beantwortet werden. Dies betraf insbesondere die Beantwortung der Fragen zur Art und Häufigkeit der Vorfälle, die eine Videoüberwachung rechtfertigen können.

Meine Mitarbeiter und ich nahmen erneut die Gelegenheit wahr, auf das Beratungsangebot meines Hauses sowie auf meine immer noch aktuellen Veröffentlichungen in den o. g. Tätigkeitsberichten zu den rechtlichen, technischen und tatsächlichen Voraussetzungen einer Videoüberwachung hinzuweisen.

10. Personalwesen

10.1
Einsatz vermeintlich kostenloser und einfach nutzbarer Technologien zur Verarbeitung von Beschäftigtendaten

Der Einsatz kostengünstiger und einfach zu implementierender Technologien in Unternehmen darf die Persönlichkeitsrechte von Arbeitnehmerinnen und Arbeitnehmern nicht beeinträchtigen. Bei unzureichender Beachtung des Datenschutzrechts kann eine solche Unternehmenspraxis schnell Verstöße nach sich ziehen.

Der Anlass

Im Frühjahr dieses Jahres erreichte mich eine Beschwerde zur Speicherung von Bewerberdaten in einem Verzeichnis eines amerikanischen Cloudspeicher- und Filehosting Dienstleisters. Die Petentin war nach Abschluss des Bewerbungsverfahrens als neue Mitarbeiterin in dem Unternehmen mit ca. 30 Mitarbeitern eingestellt worden. Nachdem sie ihre Tätigkeit aufgenommen hatte, stellte sie fest, dass die Bewerbungsunterlagen aus dem zurückliegenden und sie betreffenden Bewerbungsverfahren unverschlüsselt in einem Verzeichnis des Dienstleisters gespeichert waren.

Rechtliche Bewertung

Die Entwicklung neuer Technologien ermöglicht es kleinen und mittelständischen Unternehmen, Prozesse einfach und kostengünstig zu optimieren. Die Auswahl an technischen Werkzeugen ist dabei groß: Vom cloudbasierten Zeiterfassungssystem, das von Mitarbeitern über eine leicht bedienbare App gepflegt werden kann, über Plattformen, die den Austausch von Daten ermöglichen, oder auch Werkzeugen zur Durchführung von Mitarbeiterbefragungen – es gibt eine Vielzahl von Anwendungen, die leicht handhabbar sind und preiswert oder gar kostenfrei durch Unternehmen genutzt werden können. Es verwundert daher nicht, dass gerade viele kleine und mittelständische Unternehmen von dem sich täglich vergrößernden Angebot an neuen Softwareentwicklungen Gebrauch machen. Die Auswahl und der Einsatz entsprechender Werkzeuge sollte aber nur mit Bedacht erfolgen: Was zunächst kostengünstig und zweckmäßig erscheint, kann intensiv in Persönlichkeitsrechte von Mitarbeitern eingreifen

und daher bei unzureichender Auseinandersetzung mit den Vorschriften des Datenschutzrechts schnell zu Anordnungen und Bußgeldern durch meine Behörde führen. § 4 Abs. 1 BDSG setzt zunächst voraus, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch das BDSG oder eine anderweitige Rechtsvorschrift erlaubt oder angeordnet ist oder der Betroffene eingewilligt hat. Sofern neue Technologien eingeführt werden sollen, die personenbezogene Daten von Beschäftigten verarbeiten, hat die verantwortliche Stelle zu prüfen, auf welche Rechtsgrundlage die geplante Implementierung gestützt werden kann. Geht es um die Verarbeitung von Mitarbeiterdaten, kommt zum Beispiel § 32 Abs. 1 BDSG als zentrale Vorschrift für den Beschäftigtendatenschutz, § 28 Abs. 1 Satz 1 Nr. 2 BDSG, sofern der Arbeitgeber eigene Geschäftszwecke verfolgt, oder auch der Abschluss einer Betriebsvereinbarung in Betracht.

§ 32 Abs. 1 BDSG

Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

§ 28 Abs. 1 BDSG

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

…

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

Ebenfalls in Betracht kommen kann in Einzelfällen auch eine Einwilligung der Beschäftigten nach § 4a BDSG, dies dürfte aber die Ausnahme sein. Denn jedenfalls das für die Wirksamkeit der Einwilligungserklärung erforderliche Tatbestandsmerkmal der Freiwilligkeit wird aufgrund des zwischen Arbeitgeber und Beschäftigten bestehenden Abhängigkeitsverhältnisses in der Regel nicht zu erfüllen sein.

§ 4a BDSG

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.
…

Auch wenn die Einführung und Nutzung eines neuen technischen Werkzeugs legitimen Zwecken dient und auf eine Rechtsgrundlage gestützt werden kann, sind für eine datenschutzkonforme Einführung weitere Gesichtspunkte zu beachten. Sofern der Anbieter des Softwareprodukts auf personenbezogene Daten von Mitarbeitern zugreifen kann, ist zu prüfen, welche datenschutzrechtliche Beziehung zwischen den Parteien hierdurch entsteht. Häufig wird es sich hierbei um eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG handeln. Bei der Auftragsdatenverarbeitung betraut das implementierende Unternehmen den Dienstleister mit der Durchführung bestimmter Datenverarbeitungsvorgänge, bleibt aber für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich. Erforderlich ist dann der Abschluss eines Auftragsdatenverarbeitungsvertrages, der den Vorgaben des § 11 Abs. 2 BDSG entspricht und die nach § 9 BDSG i. V. m. Anlage 1 vom Dienstleister einzuhaltenden technischen und organisatorischen Maßnahmen beschreiben muss. Zu beobachten ist dabei, dass die Bereitschaft auf Seiten der Dienstleister, entsprechende vertragliche Vereinbarungen abzuschließen, jedenfalls dann gering ist, wenn die Technologien kostenfrei oder kostengünstig zur Verfügung gestellt werden.

§ 11 BDSG

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

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

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

…

Neben der Auftragsverarbeitung sollte auch an eine Funktionsübertragung (Übermittlung) gedacht werden. Im Gegensatz zur Auftragsdatenverarbeitung werden bei der Übermittlung personenbezogene Daten vom Dienstleister nicht streng nach den Vorgaben des Auftraggebers verarbeitet. Es findet vielmehr ein Wechsel der datenschutzrechtlichen Verantwortlichkeit statt: Mit der Übermittlung der Daten an den Dienstleister geht auch die Verantwortung auf diesen über. Bei der Übermittlung personenbezogener Daten an den Dienstleister handelt es sich gemäß § 4 Abs. 1 Satz 2 Nr. 3 BDSG um einen Unterfall der Verarbeitung personenbezogener Daten, der aufgrund des § 4 Abs. 1 BDSG ebenfalls einer Rechtsgrundlage bedarf.

Schließlich ist zu beachten, dass die Verarbeitung personenbezogener Daten bei der Nutzung neuer oder cloudbasierter Technologien häufig außerhalb Europas stattfindet. Dies hat zur Folge, dass die zum freien Datenverkehr innerhalb der Europäischen Union geschaffenen Privilegien nicht zur Anwendung gelangen. Die verantwortliche Stelle muss somit zusätzlich prüfen, ob in dem Drittstaat ein angemessenes Datenschutzniveau vorhanden ist oder zusätzliche Garantien zwischen den Parteien zu vereinbaren sind, damit die Daten auch außerhalb der EU ein dem europäischen Datenschutzrecht entsprechenden Schutz genießen.

Im vorliegenden Beschwerdefall erfolgte die Nutzung des Cloudspeicher-und Filehosting Dienstleisters ohne den Abschluss notwendiger datenschutzrechtlicher Verträge und ohne Prüfung der vorstehend dargestellten Voraussetzungen. Ich habe eine unbefugte Datenverarbeitung im Sinne von § 43 Abs. 2 BDSG festgestellt.

Es bleibt somit festzuhalten, dass die für Unternehmen zunächst kostengünstig und einfach erscheinende Implementierung neuer Technologien bei Nicht-Beachtung der zuvor skizzierten datenschutzrechtlichen Anforderungen Bußgeldtatbestände nach § 43 BDSG verwirklicht. Vor dem Hintergrund der unmittelbaren Anwendbarkeit der DS-GVO und des hiermit einhergehenden deutlich höheren Bußgeldkatalogs sollten Unternehmen sich vor Implementierung neuer technischer Werkzeuge eingehend mit den Bestimmungen des Datenschutzrechts auseinandersetzen.

11. Unternehmen, Handel und Gewerbe, Glücksspiel

11.1
Ausweiskopien beim Einchecken in Hotels

Nicht wenige Hotels fertigen beim Check-In routinemäßig Kopien von Ausweisdokumenten ihrer Gäste an. Dies wird zumeist mit vermeintlich bestehenden melderechtlichen Pflichten begründet. Tatsächlich ist das Kopieren von Ausweisen zu diesem Zweck aber weder erforderlich noch zulässig.

Der Anlass

Im Berichtszeitraum erreichten mich mehrere Eingaben, die stets den Fall betrafen, dass die jeweils Betroffenen beim Einchecken in ein Hotel vom Hotelpersonal aufgefordert wurden, ein Ausweisdokument, meist den Personalausweis, zur Anfertigung einer Kopie zu übergeben. In allen Fällen wurde dies den Gästen gegenüber mit angeblich bestehenden melderechtlichen Pflichten begründet.

Rechtliche Bewertung

Tatsächlich ist das Kopieren von Ausweisdokumenten zwar nicht generell verboten, es ist zur Erfüllung von Meldepflichten bei Hotelübernachtungen jedoch nicht erforderlich und daher auch datenschutzrechtlich nicht zulässig. Etwas anderes gilt lediglich dann, wenn der Gast ausdrücklich und freiwillig in die Erstellung der Kopie einwilligt.

Die Meldepflichten für kurzzeitige Aufenthalte in Beherbergungsstätten ergeben sich aus § 29 Abs. 2 und 3 i. V. m. § 30 des Bundesmeldegesetzes (BMG). Danach haben beherbergte Personen am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben, der ausschließlich die in § 30 Abs. 2 BMG aufgeführten Daten enthält. Lediglich bei beherbergten ausländischen Personen ist im Meldeschein die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers aufzuführen.

Zudem haben sich nur ausländische Gäste bei der Anmeldung gegenüber den Leitern der Beherbergungsstätten durch die Vorlage eines gültigen Identitätsdokumentes (anerkannter

und gültiger Pass oder Passersatz) auszuweisen und die Leiter der Beherbergungsstätten haben die Angaben im Meldeschein mit denen des Identitätsdokumentes zu vergleichen. Für inländische Gäste gelten diese Anforderungen hingegen nicht.

Weder für ausländische noch für inländische Gäste ist ein gesetzliches Erfordernis zur Anfertigung von Ausweiskopien vorgesehen.

Somit ist die Anfertigung von Ausweiskopien, ebenso wie die Vorlage des Ausweises bei inländischen Gästen, zur Erfüllung der Meldepflichten nicht erforderlich. Die Erhebung und Speicherung der auf dem Ausweis enthaltenen personenbezogenen Daten zu diesem Zweck ist daher datenschutzrechtlich unzulässig.

Ausweiskopien dürfen lediglich dann angefertigt werden, wenn der jeweilige Gast ausdrücklich und freiwillig darin eingewilligt hat. Auch die Vorlage eines Ausweises kann bei inländischen Gästen nur auf freiwilliger Basis verlangt werden.

Die jeweiligen Hotels wurden auf die geltende Rechtslage hingewiesen und verzichten zukünftig auf die Anfertigung von Ausweiskopien.

11.2
Aufzeichnung von Telefongesprächen durch Kunden-Hotlines

Viele Unternehmen möchten auf ihren Hotlines geführte Telefongespräche mit Kunden aufzeichnen. Zumeist soll dies Zwecken der Qualitätssicherung und der Schulung dienen. Eine solche Aufzeichnung ist in aller Regel nur dann zulässig, wenn die Personen, deren Gespräch aufgezeichnet wird, darin eingewilligt haben.

Ich wurde durch einen Betroffenen darauf aufmerksam gemacht, dass die auf einer bestimmten Kundenhotline eines großen Elektronikkonzerns geführten Telefongespräche zu Zwecken der Schulung und der Qualitätssicherung aufgezeichnet würden. Die Anrufer hätten jedoch keine Möglichkeit, dies zu verhindern, stattdessen würden sie per Ansage dazu aufgefordert, den Anruf zu beenden, falls sie mit der Aufzeichnung nicht einverstanden wären.

Das Unternehmen betreibt eine Vielzahl von Telefonhotlines für verschiedene Zwecke. Bei einigen davon werden die mit den Kunden geführten Gespräche aufgezeichnet. Dabei war jedoch nicht einheitlich geregelt, wie die Anrufer auf die Aufzeichnung hingewiesen werden

und auf welche Weise sie dieser widersprechen konnten. Tatsächlich gab es daher einzelne Hotlines, bei denen den Anrufern keine Möglichkeit zum Widerspruch gegen die Aufzeichnung eingeräumt wurde.

Es gibt keine gesetzliche Grundlage, die die Aufzeichnung von Telefongesprächen zu Zwecken der Schulung und der Qualitätssicherung erlaubt. Daher dürfen Telefonate zu diesen Zwecken nur aufgezeichnet werden, wenn die Anrufer dem bewusst und erkennbar zugestimmt haben oder ihnen zumindest eine Möglichkeit gegeben wird, der Aufzeichnung wirksam zu widersprechen. Zudem müssen die Anrufer vor Beginn der Aufzeichnung über diese informiert und über deren Zwecke unterrichtet werden. Wird die Einwilligung vom Anrufer nicht erteilt bzw. widerspricht dieser der Aufzeichnung, muss die verantwortliche Stelle sicherzustellen, dass tatsächlich keine Aufzeichnung erfolgt.

Aufgrund meiner Intervention wurde in dem betreffenden Unternehmen zunächst überprüft, inwiefern bei den verschiedenen Hotlines überhaupt eine Aufzeichnung geboten bzw. sinnvoll ist. Bei einigen Hotlines wird inzwischen ganz auf die Aufzeichnung von Gesprächen verzichtet. Soweit bei bestimmten Hotlines weiterhin Gespräche aufgezeichnet werden sollen, wurde ein einheitliches System eingeführt, mit dem die Zustimmung der Anrufer in datenschutzfreundlicher Weise eingeholt wird. So werden die Anrufer nunmehr zu Beginn des Telefonats durch eine automatische Ansage über die gewünschte Aufzeichnung zu bestimmten Zwecken informiert. Die Anrufer werden sodann dazu aufgefordert, durch Drücken einer Zifferntaste auf ihrem Telefon der Aufzeichnung zuzustimmen. Nur wenn die entsprechende Taste vom Anrufer gedrückt wird, wird das Gespräch auch aufgezeichnet. Wird die Taste hingegen nicht innerhalb von einigen Sekunden gedrückt, gilt die Zustimmung des Anrufers als nicht erteilt und es findet keine Aufzeichnung statt.

Auf diese Weise werden die Anrufer auf den Hotlines des Unternehmens nun transparent auf eine mögliche Aufzeichnung des Gesprächs hingewiesen und haben die Möglichkeit, sich ausdrücklich dafür oder dagegen zu entscheiden.

11.3
Videoüberwachung nach § 6b Bundesdatenschutzgesetz

Nicht zuletzt aufgrund anhaltender politischer Diskussionen und des Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen groß-

flächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz) – ist die Videoüberwachung nach dem Bundesdatenschutzgesetz (BDSG) nach wie vor Gegenstand einer Vielzahl von Eingaben, welche mich erreichen.

Durch das am 05.05.2017 in Kraft getretene Videoüberwachungsverbesserungsgesetz wurde § 6b BDSG dahingehend geändert, dass die Zulässigkeitsvoraussetzungen für die Videoüberwachung öffentlich zugänglicher Bereiche durch § 6b Abs. 1 S. 2 BDSG erweitert wurden.

So gilt bei der Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

§ 6b BDSG

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

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

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

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

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

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Absatz 1 Satz 2 gilt entsprechend.

Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

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

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

In der Gesetzesbegründung (s. BTDrucks. 18/10941) heißt es u. a.:
„… *Insofern können die Betreiber solcher Anlagen, Einrichtungen und Fahrzeuge in ihrem eigenen Interesse einen Beitrag zur Sicherheit der aufhältigen Personen leisten, der auch im öffentlichen Interesse liegt.*
Damit stehen der Polizei und Staatsanwaltschaft verstärkt effektive Übersichts-, Aufklärungs- und Ermittlungsmöglichkeiten zur Verfügung, gerade wenn es darum geht, unmittelbar reagieren zu können. …“

Die „Quasi-Übertragung hoheitlicher Aufgaben“ – Videoüberwachung öffentlich zugänglicher Bereiche durch Private an Stelle der Polizei und Staatsanwaltschaft – stieß im Laufe des Gesetzgebungsverfahrens auf laute Kritik seitens der Aufsichtsbehörden. In der Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Kühlungsborn vom 09.11.2016 wurden diese zum Ausdruck gebracht, allerdings im weiteren Verlauf des Gesetzgebungsverfahrens nicht berücksichtigt.

Auf meine Tätigkeit im aktuellen Berichtszeitraum hatte das Videoüberwachungsverbesserungsgesetz bislang keine nennenswerten Auswirkungen.

Im weit überwiegenden Teil der mich erreichenden Eingaben geht es nach wie vor um den klassischen Nachbarschaftsstreit, Gewerbetreibende, die weit mehr als ihr eigenes Firmengelände überwachen, sowie Bürgerinnen und Bürger, die in Unkenntnis der Rechtslage Kamerasysteme installieren, die weitaus mehr als nur das Privatgrundstück im Fokus haben. In allen Fällen des Berichtszeitraums konnte – in Zusammenarbeit mit den Kamerabetreibern – ein datenschutzkonformer Betrieb der Überwachungsanlagen hergestellt werden. Positiv hervorzuheben ist erneut, dass viele Kamerabetreiber bereits vor deren Installation das Gespräch

mit meiner Behörde suchen, sodass von vornherein ein datenschutzkonformer Betrieb sichergestellt werden kann.

Wie sich die Videoüberwachung öffentlich zugänglicher Bereiche entwickelt, ist aktuell nicht absehbar, insbesondere vor dem Hintergrund, dass die ab 25.05.2018 anzuwendende Datenschutz-Grundverordnung (DS-GVO) explizit keinerlei Regelung diesbezüglich enthält.

Bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche verlangt Art. 35 Abs. 3c DS-GVO lediglich eine Datenschutz-Folgenabschätzung. Die Zulässigkeitsvoraussetzungen werden aus Art. 6 Abs. 1 S. 1 DS-GVO i. V. m. Art. 5 DS-GVO abzuleiten sein.

Art. 35 Abs. 3c DS-GVO

Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) ...
b) ...
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Art. 6 Abs. 1 Satz 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.

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben 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; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („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“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Welche konkreten Auswirkungen dies auf die aufsichtsbehördliche Praxis hat, wird sich erst im Laufe des kommenden Jahres zeigen.

11.4
Anschluss geduldeter Sportwettenanbieter und Sportwettenvermittler an die Spielersperrdatei OASIS

Aus datenschutzrechtlicher Sicht können nicht nur konzessionierte, sondern auch von den Aufsichtsbehörden geduldete Anbieter und Vermittler von Sportwetten an OASIS angeschlossen werden.

Ein Unternehmen bat mich, datenschutzrechtlich zu überprüfen, ob geduldete Sportwettenanbieter und Sportwettenvermittler an die Spielersperrdatei OASIS angeschlossen werden dürfen. Zum Schutz der Spieler und zur Bekämpfung der Spielsucht haben die Länder ein bundesweites Sperrsystem eingerichtet, an dem sich Spielbanken sowie Veranstalter und Vermittler von Sportwetten und von Lotterien mit besonderem Gefährdungspotential beteiligen müssen. In die Sperrdatei werden die Spieler eingetragen, die nach dem Glückspielstaatsvertrag (GVBl. 2012, 190, 197) nicht am Spielbetrieb einer Spielbank, an Sportwetten oder bestimmten Lotterien teilnehmen dürfen. Das Land Hessen hat das Spielersperrsystem „OASI GlüStV“ (Onlineabfrage Spielerstatus nach Glücksspielstaatsvertrag) aufgebaut und führt die zentrale Sperrdatei. Der Betrieb erfolgt durch die Hessische Zentrale für Datenverarbeitung (HZD).

Geduldete Sportwettenanbieter und Sportwettenvermittler

Die Glücksspielaufsicht sieht sich wegen anhängiger Gerichtsverfahren gegenwärtig nicht in der Lage, Konzessionen zum Veranstalten und Vermitteln von Sportwetten zu erteilen. Angesichts der zu erwartenden langen Dauer der Verfahren und der europarechtlichen Verpflichtung, das deutsche Sportwettenmonopol des Staates zu beseitigen und privaten Anbietern die Veranstaltung und Vermittlung von Sportwetten zu ermöglichen, haben sich die Aufsichtsbehörden auf eine Übergangslösung verständigt.

Die Bundesländer haben zu diesem Zweck Leitlinien für eine Duldung des Veranstaltens und Vermittelns von Sportwetten entwickelt, die sich an den materiellen Voraussetzungen für den Erhalt einer Konzession orientieren. Veranstalter und Vermittler von Sportwetten, die die Anforderungen nach § 4a GlüStV erfüllen, können statt einer Erlaubnis eine Duldung erhalten. Rechtsgrundlage dafür ist § 9 Abs. 1 Satz 2 GlüStV i. V. m. den entsprechenden Vorschriften der Bundesländer. Die Duldung stellt bei einem formell wegen fehlender Erlaubnis illegalen Sportwettenangebot, das materiell erlaubnisfähig ist, das ermessensfehlerfreie „Minus“ zur Untersagungsverfügung nach § 9 Abs. 1 Nr. 3 GlüStV dar (OVG Schleswig-Holstein, Beschluss vom 04.05.2015, Az. 2 MB 1/15, Rdnr. 17). Die Rechtmäßigkeit dieser Duldungspraxis in Rheinland-Pfalz hat das Bundesverwaltungsgericht in seinem Beschluss vom 22.07.2014 (Az. 8 B 86/13) anerkannt. Entscheidend ist, dass sichergestellt wird, dass Sportwetten nur durch zuverlässige Personen vermittelt werden, die einen ordnungsgemäßen, den gesetzlichen Vorgaben entsprechenden Vertrieb der Wettangebote gewährleisten (OVG Schleswig-Holstein, a. a. O., Rdnr. 15).

Zur materiellen Erlaubnisfähigkeit als Voraussetzung für eine Duldung nach § 9 Abs. 1 Satz 2 GlüStV gehört auch, dass durch eine Abfrage im Spielersperrsystem OASIS gewährleistet wird, dass gesperrte Spieler vom Wettbetrieb ausgeschlossen bleiben (§ 21 Abs. 5 GlüStV) und Veranstalter von Sportwetten Spielersperren im System eintragen und verwalten (§ 8 Abs. 4 GlüStV). Vermittler haben an dem Sperrsystem mitzuwirken (§ 8 Abs. 6 Satz 1 GlüStV). Sowohl Veranstalter als auch Vermittler haben durch eine Onlineabfrage des Spielerstatus bei der Spielersperrdatei OASIS sicherzustellen, dass keine gesperrten Spieler an Sportwetten teilnehmen.

§ 21 Abs. 5 GlüStV

Gesperrte Spieler dürfen an Wetten nicht teilnehmen. Die Durchsetzung des Verbots ist durch Kontrolle des Ausweises oder eine vergleichbare Identitätskontrolle und Abgleich mit der Sperrdatei zu gewährleisten.

§ 8 Abs. 4 GlüStV

Die Veranstalter haben die in § 23 Abs. 1 genannten Daten in eine Sperrdatei einzutragen. Ein Eintrag ist auch zulässig, wenn nicht alle Daten erhoben werden können.

§ 8 Abs. 6 Satz 1 GlüStV

Zum Schutz der Spieler und zur Bekämpfung der Glücksspielsucht sind die Vermittler von öffentlichen Glücksspielen verpflichtet, an dem übergreifenden Sperrsystem (§ 23) mitzuwirken.

Geduldete Veranstalter von Sportwetten erhalten daher einen lesenden und schreibenden Zugriff auf OASIS. Sportwettenvermittler benötigen keinen schreibenden Zugriff auf die Sperrdatei, da sie keine Sperren eintragen und verwalten dürfen, sondern Anträge auf Selbstsperrung an den Veranstalter zu übermitteln haben (§ 8 Abs. 6 GlüStV). Entsprechend erhalten Vermittler nur einen lesenden Zugriff auf das Spielersperrsystem, um so ihrer Verpflichtung, gesperrte Spieler von der Teilnahme an Sportwetten auszuschließen, nachkommen zu können. Dem Vermittler werden keine Daten der gesperrten Spieler angezeigt. Bei der Eingabe von Kundendaten (Name, Vorname, Geburtsdatum) erhält der Vermittler lediglich die Mitteilung, ob eine Person mit diesen Angaben im System als gesperrt registriert ist oder nicht. Angezeigt wird nur: Spieler ist gesperrt oder Spieler ist nicht gesperrt.

Ob die von den glücksspielrechtlichen Aufsichtsbehörden ausgesprochenen Duldungen rechtmäßig sind, kann letztlich nur gerichtlich geklärt werden. Entscheidend für die datenschutzrechtliche Beurteilung ist, dass geduldete Veranstalter und Vermittler dieselben materiellen glückspielrechtlichen Anforderungen erfüllen wie ein konzessionierter Sportwettenanbieter. Deswegen genügt auch eine – wie in manchen Bundesländern praktizierte – stillschweigende Duldung ohne Prüfung, ob die materiellen Anforderungen für die Erteilung einer Erlaubnis erfüllt sind, für einen Anschluss an OASIS nicht.

Datensicherheit

Zweifellos verursacht der Anschluss einer Vielzahl von Wettvermittlungsstellen an OASIS ein zusätzliches Datensicherheitsrisiko.

Das wird zum einen jedoch bereits dadurch verringert, dass die Vermittlungsstellen keinen schreibenden Zugriff haben, sondern nur den oben dargestellten lesenden, wobei jeder Zugriff durch die HZD protokolliert wird. Zum anderen bedürfen auch Wettvermittlungsstellen einer Erlaubnis, die nur der Inhaber der Sportwettenkonzession beantragen kann (§ 10 Abs. 7 HGlüG). Entsprechend der Duldung für den Konzessionsinhaber kann auch für die Sportwettenvermittler nur eine Duldung in Betracht kommen, die voraussetzt, dass eine materielle Erlaubnisfähigkeit gegeben ist. Die Duldung bedingt, dass der Betreiber die materiellen landesrechtlichen Voraussetzungen für eine Erlaubnis erfüllt (in Hessen § 10 Abs. 8 HGlüG).

Die Erlaubnis darf in Hessen nur erteilt werden, wenn keine Tatsachen die Annahme rechtfertigen, dass der Betreiber der Wettvermittlungsstelle die für diese Tätigkeit erforderliche Zuverlässigkeit nicht besitzt (§ 10 Abs. 8 Nr. 3 HGlüG), und keine Anhaltspunkte dafür vorliegen, dass der Betreiber den Anforderungen des Jugend- und Spielerschutzes nicht hinreichend nachkommen wird (§ 10 Abs. 8 Nr. 4 HGlüG).

§ 10 Abs. 8 HGlüG

Die Erlaubnis zum Betreiben von Annahmestellen und Wettvermittlungsstellen darf nur erteilt werden, wenn

...

3. keine Anhaltspunkte die Annahme rechtfertigen, dass die Betreiberin oder der Betreiber die für diese Tätigkeit erforderliche Zuverlässigkeit nicht besitzt,
4. keine Anhaltspunkte dafür vorliegen, dass die Betreiberin oder der Betreiber den Anforderungen des Jugend- und des Spielerschutzes nicht hinreichend nachkommen wird, ...

Gemäß § 4b Abs. 2 Nr. 2 GlüStV muss der Bewerber im Konzessionsverfahren ein IT- und Datensicherheitskonzept vorlegen. Der geduldete Sportwettenanbieter hat außerdem mit seinem jährlichen Bericht an die Aufsichtsbehörde einen Prüfbericht einer externen und unabhängigen Stelle über die Einhaltung der technischen Standards und die Wirksamkeit der im Sicherheitskonzept vorgesehenen und in der Duldungsverfügung vorgeschriebenen Sicherheitsmaßnahmen vorzulegen.

§ 4b Abs. 2 Nr. 2 GlüStV

Die Bewerbung bedarf der Schriftform. Sie muss alle Angaben, Auskünfte, Nachweise und Unterlagen in deutscher Sprache enthalten, die in der Bekanntmachung bezeichnet sind, welche für die Prüfung der Voraussetzungen nach § 4a Abs. 4 erforderlich sind und die Auswahl nach Absatz 5 ermöglichen. Dazu gehören insbesondere:

...

2. eine Darstellung der Maßnahmen zur Gewährleistung der öffentlichen Sicherheit und Ordnung und der sonstigen öffentlichen Belange unter besonderer Berücksichtigung der IT- und Datensicherheit (Sicherheitskonzept), ...

Die in meinem 42. Tätigkeitsbericht (Ziff. 2.1.2.1) angesprochene, aus meiner Sicht unverhältnismäßige, damals vorgesehene Speicherdauer der Protokollierung wurde geändert. Die Aufbewahrungsfrist beträgt jetzt ein Jahr.

Ferner wird durch angemessene technische und organisatorische Maßnahmen ein Missbrauch verhindert. Eine Auswertung muss im 4-Augen-Prinzip autorisiert werden. Die Prüfung erfolgt durch das Regierungspräsidium Darmstadt und den IT-Sicherheitsbeauftragten des hessischen Innenministeriums.

Die Auswertung der Protokolle kann jeweils nur bezüglich einer Person erfolgen. Das Zugriffsrecht um eine Auswertung zu initiieren, hat das zuständige Dezernat des Regierungspräsidiums. Es müssen die Daten der damaligen Statusabfrage exakt eingegeben werden, die Veranstalterkennung muss zutreffen und zu einer zwingend einzugebenden Zeit werden die folgenden 48 Stunden abgefragt.

Sobald eine Auswertung gestartet wird, erhält der IT-Sicherheitsbeauftragte des HMDIS automatisch eine Information darüber und kann diese mit den ihn bekannten Autorisierungen abgleichen. Jede beantragte Abfrage wird beim Regierungspräsidium und beim IT-Sicherheitsbeauftragten des HMDIS dokumentiert.

Eine missbräuchliche Auswertung ist daher nicht zu erwarten.

11.5
USB-Aufnahmefunktion eines DVB-T-Empfängers

Wer vor der erstmaligen Benutzung von TV-Geräten, DVD- und Blu-ray-Playern, Satelliten- oder DVB-T-Empfängern etc. über das Gerät aufgefordert wird, dem Hersteller oder Verkäufer seinen Namen, seine Postanschrift und das Kaufdatum mitzuteilen, sollte der Aufforderung nicht folgen, denn eine derartige Datenerhebung ist unzulässig.

Durch den Hinweis eines betroffenen Verbrauchers wurde ich auf ein hessisches Unternehmen aufmerksam gemacht, das sog. DVB-T2-Empfänger (englische Abkürzung für „Digital Video Broadcasting – Terrestrial"; deutsch etwa: „Digitale Videoübertragung – Antennenfernsehen") herstellt und vertreibt, die den neuen hochauflösenden HD-Standard empfangen können, in dem seit März 2017 das digitale Antennenfernsehen in vielen deutschen Ballungsräumen ausgestrahlt wird. Diese Geräte sind oft mit USB-Buchsen und einer entsprechenden Aufnahmefunktion ausgestattet, die es ermöglicht, TV-Sendungen auf einen USB-Stick oder eine externe USB-Festplatte aufzuzeichnen und die Sendungen dann zeitversetzt oder im Nachhinein anzusehen (sog. „PVR-Funktion", englische Abkürzung für „Personal Video Recorder").

Der betroffene Verbraucher, der einen neuen DVB-T2-Empfänger des o. a. Herstellers in einem Elektronik-Fachmarkt erworben hatte, beschwerte sich nun darüber, dass diese PVR-Funktion nicht sofort funktionsfähig war, obwohl sie auf der Verpackung des Geräts beworben wurde. Stattdessen wurde ihm beim Versuch, eine externe USB-Festplatte für die PVR-Funktion zu nutzen, auf dem Bildschirm angezeigt, dass die Aufnahmefunktion derzeit nicht aktiviert sei. Um die Funktion zu aktivieren, müsse er eine bestimmte Servicetelefonnummer des Herstellers anrufen. Von dort würde er einen Freischaltcode erhalten, der dann in das Gerät einzugeben sei. Erst danach wäre die PVR-Funktion über den USB-Anschluss des DVB-T2-Empfängers benutzbar.

Beim Anruf der angegebenen Servicenummer des Herstellers wurde der Käufer damit konfrontiert, dass er dem Hersteller neben der Seriennummer und dem Produktcode des Geräts auch noch seinen Namen, seine Postanschrift und das Kaufdatum mitteilen sollte. Auf die Nachfrage, zu welchem Zweck das Unternehmen diese personenbezogenen Daten benötige, erhielt er keine zufriedenstellende Antwort. Auch der Hinweis, dass auf der Gerätepackung der Aufdruck angebracht sei, dass das Gerät über eine PVR-Funktion verfüge und dass Käufer über eine zusätzliche spätere Erhebung ihrer Daten nirgendwo unterrichtet würden, brachte

keinen Fortschritt. Ohne Angabe seiner personenbezogenen Daten wurde ihm kein Freischaltcode mitgeteilt.

Der Betroffene wandte sich daraufhin an mich und bat mich zu prüfen, ob die Erhebung und Verarbeitung dieser Käuferdaten überhaupt datenschutzrechtlich zulässig sei.

Ich forderte das Unternehmen zur Stellungnahme auf, insbesondere zur Frage, welche Interessen es mit der Datenerhebung verfolge und weshalb es erforderlich im Sinne von § 28 Abs. 1 Nr. 2 BDSG sein soll, zur PVR-Freischaltung personenbezogene Käuferdaten zu erheben und zu verarbeiten.

§ 28 BDSG

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

...

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

In seiner Antwort rechtfertigte das Unternehmen die Erhebung und Verarbeitung der Käuferdaten mit der Vorschrift in § 54 Urheberrechtsgesetz (UrhG), nach der eine Abgabe an die Zentralstelle für private Überspielungsrechte (ZPÜ, früher: GEMA) nur für die Geräte zu entrichten sei, bei denen die USB-Aufnahmefunktion auch benutzt wird. Die Erhebung der Daten der Käufer sei zwingend erforderlich, um der ZPÜ revisionssicher Auskunft über die Zahl der an den Markt gebrachten Geräte mit aktivierter Aufnahmefunktion geben zu können. Auch ein mit der Unternehmensrevision beauftragter externer Wirtschaftsprüfer würde diese Datenerhebung und -verarbeitung für notwendig halten.

Diese Begründung konnte schon deswegen nicht überzeugen, weil eine telefonische Datenerhebung ohne weitere Verifikation der angegebenen Daten nie wirklich revisionssicher sein kann. Zur Erhebung der Zahl der betroffenen verkauften Geräte, bei denen die PVR-Funktion freigeschaltet werden soll, wäre es schließlich auch durchaus ausreichend, sich vor der Übermittlung des Freischaltcodes nur die Seriennummer und den Produkt-Code des gekauften Geräts ohne die personenbezogenen Daten des Käufers nennen lassen. Das Herstellerunternehmen hatte ja offensichtlich keine Möglichkeit nachzuvollziehen, ob ihm korrekte Daten oder falsche Daten von den Betroffenen am Telefon genannt werden. Jeder Anrufer könnte an der

Servicetelefonnummer irgendeinen Namen und irgendeine Postanschrift nennen. Daher kann die vorliegende Datenerhebung und -verarbeitung auch nichts zu einer Revisionssicherheit beitragen, und zwar weder gegenüber der ZPÜ noch für einen beauftragten Wirtschaftsprüfer. Eine datenschutzrechtliche Erforderlichkeit gemäß § 28 Abs. 1 Nr. 2 BDSG für diese Datenerhebung und -verarbeitung war schon deswegen kaum zu begründen.

Meine Nachfrage bei der ZPÜ ergab jedoch zudem, dass sich die von der ZPÜ nach § 54 UrhG geltend gemachten Auskunfts- und Vergütungsansprüche auf sämtliche Geräte erstrecken, die über eine Vervielfältigungsfunktion verfügen. Es kommt also nicht darauf an, ob diese Funktion bereits beim Verkauf freigeschaltet ist oder erst zu einem späteren Zeitpunkt vom Käufer freigeschaltet werden muss. Der ZPÜ ist die Gesamtzahl der auf den Markt gebrachten Geräte zu melden, unabhängig davon, ob die PVR-Funktion nach dem Kauf noch freigeschaltet werden muss oder nicht. Die ZPÜ hat mir weiterhin mitgeteilt, dass von ihr daher auch in keinem Fall eine Nennung von Namen oder Anschriften von Personen von den Hersteller- oder Vertriebsfirmen entsprechender Geräte verlangt wird.

Die Datenerhebung und -verarbeitung war also eindeutig nicht erforderlich im Sinne von § 28 Abs. 1 Nr. 2 BDSG. Eine andere datenschutzrechtliche Rechtsgrundlage im Sinne von § 4 Abs. 1 BDSG, die hierfür in Frage kommen könnte, war nicht erkennbar. Das Verfahren der Erhebung und Verarbeitung personenbezogener Daten bei der Freischaltung der PVR-Funktion der an den Markt gebrachten DVB-T-Empfänger war folglich datenschutzrechtlich unzulässig.

Ich habe das Unternehmen daher aufgefordert, die Erhebung personenbezogener Daten der Käufer von entsprechenden Geräten mit USB-Aufnahmefunktion umgehend einzustellen. Bei Käufern von bereits in den Markt gebrachten Geräten, die die PVR-Funktion künftig freischalten möchten, genügt es, diese nach der Seriennummer und dem Produktcode zu fragen, um ihnen den passenden Freischalt-Code zu übermitteln.

Weiterhin wurde dem Unternehmen aufgegeben, alle bislang in diesem Zusammenhang in der Vergangenheit bereits erhobenen und gespeicherten personenbezogenen Daten zu löschen, da es für die weitere Speicherung dieser Daten keine Rechtsgrundlage gibt. Das Unternehmen zeigte sich einsichtig und sagte mir die sofortige Änderung seiner Geschäftsprozesse zur PVR-Freischaltung sowie die Löschung der bereits erhobenen Daten zu.

12. Internet und Online-Shops

12.1
E-Mail-Versandbenachrichtigungen durch Paketdienstleister

Viele Onlinehändler übermitteln die E-Mail-Adressen ihrer Kunden an den mit dem Versand der gekauften Ware beauftragten Paketdienstleister, damit dieser die Kunden über den Empfang des Pakets informieren kann. Dies liegt in aller Regel im Interesse aller Beteiligten und ist datenschutzrechtlich zulässig.

Mich erreichten mehrere Eingaben, in denen Kunden von Onlinehändlern die Weitergabe ihrer E-Mail-Adresse an den jeweiligen Versanddienstleister kritisierten und die Zulässigkeit dieser Datenübermittlung anzweifelten.

Beim Onlineshopping ist es üblich, dass die Kunden über den Versand der bestellten Waren per E-Mail informiert werden. Dies passiert häufig durch den Onlinehändler selbst. Dieser kann jedoch lediglich darüber informieren, dass die Waren sein Lager verlassen haben. Den Transport und die Zustellung der Waren übernehmen in aller Regel vom Händler beauftragte Versanddienstleister.

Nur diese können die Kunden auch über Details zum Versand informieren, z. B. zum geplanten Zustellungszeitpunkt. Um dies zu ermöglichen, geben inzwischen viele Onlinehändler auch die E-Mail-Adressen ihrer Kunden an den beauftragten Versanddienstleister weiter. Auf diese Weise kann dieser mit den Kunden bzw. Paketempfängern Kontakt aufnehmen, sie über den Versand informieren und ggf. weitere Modalitäten der Zustellung vereinbaren (z. B. Wunsch-Zustellungstermin, Abgabe bei Nachbarn etc.).

Selbstverständlich muss und darf ein Onlinehändler dem von ihm beauftragten Versanddienstleister die Namen und Anschriften seiner Kunden mitteilen, da ohne diese Informationen die Zustellung der Ware nicht möglich wäre. Die E-Mail-Adresse eines Kunden wird dagegen üblicherweise nicht benötigt, um ein Paket zuzustellen. Lediglich in Ausnahmefällen, z. B. beim Versand von Waren durch Speditionen, kann die Kontaktaufnahme des Versanddienstleisters mit dem Kunden erforderlich sein, um beispielsweise einen Liefertermin zu vereinbaren.

Dennoch liegen die Benachrichtigung des Paketempfängers durch den Versanddienstleister und die damit verbundene Eröffnung einer Kontaktmöglichkeit zwischen diesen Beteiligten in

aller Regel im Interesse sowohl des Onlinehändlers, des Versanddienstleisters als auch des Empfängers/Kunden selbst.

Der Händler kann mit der Versandbenachrichtigung einen zusätzlichen Service anbieten und verringert zudem die Gefahr, dass Pakete an ihn zurücklaufen, die nicht ausgeliefert werden konnten. Für den Versanddienstleister wird die Auslieferung erleichtert, da die Empfänger sich auf den Liefertermin einstellen oder Alternativen dazu auswählen können. Somit dient die Kontaktaufnahme des Versanddienstleisters mit dem Paketempfänger per E-Mail der erfolgreichen Auslieferung und damit auch der Erfüllung des Kaufvertrags mit dem Händler. Dies ist umso wichtiger z. B. bei verderblicher Ware oder bei zeitkritischen Lieferungen.

Dagegen besteht regelmäßig kein Grund zur Annahme, dass ein schutzwürdiges Interesse des Paketempfängers am Ausschluss der Übermittlung seiner E-Mail-Adresse die Interessen des Händlers und des Versanddienstleisters überwiegt. Vielmehr wünschen die meisten Kunden von Onlineshops sogar genauere Informationen zur Zustellung ihres Pakets bzw. die Auswahl von Zustellungsalternativen. Zudem unterliegen die Versanddienstleister zur Wahrung des Postgeheimnisses besonderen datenschutzrechtlichen Verpflichtungen.

Onlinehändler dürfen somit beim Versand von Waren die E-Mail-Adresse des jeweiligen Kunden an den Versanddienstleister übermitteln, damit dieser den Kunden kontaktieren und über die Paketzustellung informieren kann.

12.2
Plötzlich Kunde ohne eigenes Zutun? Vom Sinn der Auskunft nach § 34 Abs. 1 BDSG

Das Recht auf Auskunft über die zur Person gespeicherten Daten ist eines der wichtigsten Instrumente für Betroffene, datenschutzrechtliche Ansprüche bei verantwortlichen Stellen geltend zu machen. Oft eröffnet die erteilte Auskunft den Weg zur Berichtigung falscher Angaben oder zur Löschung unzulässig gespeicherter Daten. Darüber hinaus können anlässlich einer solchen „Selbstauskunft" sogar strukturelle Fehler in Geschäftsprozessen und Datenverarbeitungssystemen verantwortlicher Stellen entdeckt und behoben werden.

Ein Betroffener wandte sich an mich, da er immer wieder unerwünschte Werbe-E-Mails eines ihm unbekannten Online-Portals aus der Touristik-Branche erhalten hatte, dessen Betreiber seinen Sitz in Hessen hat. Über dieses Online-Portal können Urlauber weltweit Zimmer sowie

Ferienwohnungen und -häuser recherchieren und buchen. Auf seine Nachfrage im Sinne von § 34 Abs. 1 BDSG, welche Daten dem Unternehmen zu seiner Person vorliegen und woher diese Daten stammen, sowie auf seine Aufforderung, alle vorhandenen Daten zu seiner Person umgehend zu löschen und den Versand von Werbe-E-Mails zu unterlassen, habe er keine Antwort erhalten. Stattdessen habe das Unternehmen seine E-Mail-Adresse weiterhin zur Versendung von Werbe-E-Mails und Kundenmitteilungen verarbeitet und genutzt.

Ich habe das Unternehmen daraufhin aufgefordert, zu dem Vorgang Stellung zu nehmen und einige sich daraus ergebende Fragen zur Verarbeitung personenbezogener Daten zu Werbezwecken und zur Auskunftserteilung an Betroffene zu beantworten. Dabei habe ich insbesondere darauf hingewiesen, dass die Nichtbeachtung des Auskunftsanspruchs von Betroffenen entgegen § 34 Abs. 1 BDSG den Bußgeldtatbestand des § 43 Abs. 1 Nr. 8a BDSG erfüllt. Zudem habe ich den Anbieter des Online-Portals zur Löschung der Daten des Betroffenen aus seinen EDV-Systemen nach erfolgter Beauskunftung aufgefordert.

§ 34 Abs. 1 BDSG

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

§ 43 Abs. 1 Nr. 8a BDSG

Ordnungswidrig handelt, wer vorsätzlich
...
8a. entgegen § 34 Absatz 1 Satz 1 […] eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,
…

Das Unternehmen reagierte darauf umgehend und stellte zunächst dar, dass es durch die Neubestellung eines fachkundigen und kompetenten externen betrieblichen Datenschutzbeauftragten in der Übergangszeit leider zu unerwünschten Verzögerungen bei der Bearbeitung

datenschutzrelevanter Vorgänge gekommen sei. Der neue betriebliche Datenschutzbeauftragte habe sich aber inzwischen gut eingearbeitet und habe die Probleme mittlerweile behoben, indem er die entsprechenden Geschäftsprozesse zur Erteilung von Selbstauskünften an Betroffene den Erfordernissen des Datenschutzrechts angepasst habe.

Beigefügt war auch eine ausführliche Auskunft gem. § 34 Abs. 1 BDSG für den Betroffenen, der zu entnehmen war, dass der Betroffene schon vor Monaten über die Vermittlung des Online-Portals ein Ferienhaus eines Vermieters für einen Kurzurlaub an der Nordsee gebucht hatte. Die Auskunft enthielt wie gesetzlich vorgeschrieben alle vorliegenden Detaildaten, wie Name, Anschrift, E-Mail-Adresse, Telefonnummer, Buchungszeitpunkt, gebuchtes Objekt, genaue Reisedaten, Anzahl der Reisenden und Mietpreis. Die Daten des Betroffenen würden daher nicht gelöscht, sondern zur Erfüllung des Vertragszwecks gem. § 28 Abs. 1 BDSG notwendigerweise weiterverarbeitet. Dieser wolle ja schließlich in Kürze seinen gebuchten Nordseeurlaub genießen. Der Widerspruch gegen die Verarbeitung der E-Mail-Adresse des Betroffenen zu Werbezwecken werde ab sofort beachtet. E-Mails im Zusammenhang mit seiner Buchung werde der Betroffene aber im Sinne von § 28 Abs. 1 Nr. 1 BDSG selbstverständlich weiterhin erhalten.

§ 28 Abs. 1 Nr. 1 BDSG

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig
1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Nachdem ich diese an sich schlüssigen Angaben an den Betroffenen weitergeleitet hatte, widersprach dieser zu meiner Überraschung der Auskunft des Unternehmens mit großem Nachdruck und bestand weiter darauf, das Online-Portal nie genutzt zu haben. Er habe hingegen seinen Nordsee-Urlaub über die dortige lokale Tourismus-Zentrale organisiert und habe über diese Stelle auch das Ferienhaus des Vermieters gebucht. Dies konnte er auch durch Vorlage geeigneter Unterlagen belegen. Die o. a. Detaildaten des Urlaubs, die ihm beauskunftet wurden, seien allerdings alle korrekt, was für ihn die Frage aufwerfe, wie das Online-Portal an seine sämtlichen Urlaubsdaten gelangt war. Er habe deshalb bereits die Suche nach einem Datenleck in der dortigen lokalen Tourismus-Zentrale veranlasst.

Ich habe das hessische Portal-Unternehmen daraufhin mit den Angaben des Betroffenen konfrontiert und den neu bestellten betrieblichen Datenschutzbeauftragten aufgefordert, Nachforschungen in dem Unternehmen anzustellen, um den vorliegenden Widerspruch über die Datenherkunft aufzuklären.

Nach intensiven internen Untersuchungen und Überprüfungen der jeweiligen Datenquellen und Datenflüsse in den verteilten Datenbanken des Unternehmens konnte der betriebliche Datenschutzbeauftragte die Ursache der aufgetretenen Widersprüche ermitteln und auch erklären, wie das Online-Portal an die korrekten Urlaubsdaten des Betroffenen gelangt war: Er hatte nämlich herausgefunden, dass der Vermieter des Ferienhauses seine Objekte über mehrere Online-Portale und Vermittler angeboten hatte. Bei gelungener Vermietung verwaltete der Vermieter seine Objekte aber immer über die Online-Kalenderfunktion des hessischen Online-Portalanbieters, auch wenn die Vermittlung ursprünglich über einen anderen Anbieter stattfand. Für den Zeitraum der Vermietung wurde das Objekt hierdurch für die Vermittlung in dem Portal blockiert, was Doppelbuchungen verhinderte. Dieser Vermieter-Online-Kalender war allerdings EDV-technisch an das kaufmännische Buchungssystem des Portalanbieters gekoppelt. Dies hatte zur Folge, dass der Portalanbieter die vom Vermieter im Online-Kalender eingegeben Daten als eigene Daten verarbeitete und den Betroffenen genauso wie einen eigenen Online-Kunden behandelte.

Nachdem diese fehlerhafte Datenverarbeitung festgestellt und von mir ausdrücklich beanstandet wurde, löschte der Portalanbieter die Daten des Betroffenen komplett aus seinen Systemen und traf softwareseitig geeignete technisch-organisatorische Maßnahmen, um den Vermieterkalender vom Buchungssystem zu entkoppeln, sodass Irritation und Falschverarbeitungen wie in diesem Fall künftig nicht mehr entstehen können.

12.3
Zugriff auf den internen Bereich einer Gewerkschafts-Webseite

Viele Webseiten haben für einen begrenzten Personenkreis (z. B. Mitglieder eines Vereins, Kunden eines Unternehmens) einen internen Bereich, in dem diese ihre personenbezogenen Daten einsehen und ändern können. Der Zugang zu solchen Bereichen muss technisch so abgesichert sein, dass Zugriffe von unberechtigten Personen ausgeschlossen sind.

Durch eine Eingabe wurde ich darauf aufmerksam, dass eine große Gewerkschaft mit Sitz in Hessen auf ihrer Webseite einen internen Bereich zur Verfügung stellt, in dem die Gewerkschaftsmitglieder u. a. Änderungen ihrer Daten mitteilen und bestimmte Dienste (z. B. ein Diskussionsforum) nutzen können.

Eine spezielle Anmeldung bzw. Registrierung für die Nutzung des internen Bereichs war nicht vorgesehen, vielmehr wurde mit Eintritt in die Gewerkschaft automatisch ein individueller Account für jedes Mitglied eingerichtet. Der Zugang zum internen Bereich erfolgte allein anhand der Eingabe der Mitgliedsnummer und des Geburtsdatums des jeweiligen Mitglieds. Eine Änderung dieser Login-Daten war nicht möglich.

Diese Form der Zugriffsbeschränkung war jedoch nicht ausreichend, um sicherzustellen, dass nur die berechtigten Gewerkschaftsmitglieder Zugriff auf den internen Bereich der Webseite und damit auch auf ihre personenbezogenen Daten hatten. Das Geburtsdatum einer Person ist üblicherweise einem größeren Personenkreis bekannt. Die Gewerkschafts-Mitgliedsnummer ist zwar regelmäßig kaum anderen Personen als dem Mitglied selbst bekannt, allerdings ist diese erkennbar auf den Adressaufklebern der monatlich versandten Mitgliederzeitschrift der Gewerkschaft aufgedruckt. Somit war es zumindest einem nicht ganz kleinen Personenkreis, der das Geburtsdatum eines Gewerkschaftsmitglieds kannte und eine physische Zugriffsmöglichkeit auf dessen Gewerkschaftszeitung hatte, problemlos möglich, sich in dessen Namen auf der Webseite einzuloggen und die Dienste zu nutzen bzw. die zur Person gespeicherten Daten zu ändern.

Zudem wurde bei allen im internen Bereich der Webseite getätigten Beiträgen (z. B. im Diskussionsforum) automatisch der volle Name des jeweiligen Mitglieds genannt. Dies widerspricht jedoch der Anforderung des § 13 Abs. 6 S. 1 TMG, wonach generell eine pseudonyme Nutzungsmöglichkeit von Internetdiensten ermöglicht werden soll.

Auf meine Aufforderung hat die Gewerkschaft inzwischen den Login-Prozess zum internen Bereich der Webseite geändert. Nunmehr ist zu dessen Nutzung eine einmalige Registrierung erforderlich, bei der die Gewerkschaftsmitglieder neben der weiterhin erforderlichen Angabe ihrer Mitgliedsnummer und ihres Geburtsdatums einen Benutzernamen und ein eigenes Passwort vergeben müssen. Die Anmeldung zum internen Bereich der Webseite kann nur noch mit dem selbst vergebenen Benutzernamen und Passwort erfolgen. Auf diese Weise ist die Missbrauchsgefahr minimiert und die Gewerkschaftsmitglieder können durch die Vergabe eigener Zugangsdaten sicherstellen, dass keine unberechtigten Personen ihren Account nutzen können.

Zudem werden anderen Nutzern innerhalb des internen Bereichs der Webseite nur noch die selbst gewählten Benutzernamen und nicht mehr die echten Namen anderer Nutzer angezeigt. Sofern ein Gewerkschaftsmitglied die Dienste nicht unter seinem echten Namen nutzen möchte, kann dies durch die Wahl eines pseudonymen Benutzernamens vermieden werden.

13. Kreditinstitute, Banken, Auskunfteien, Versicherungswirtschaft

13.1
Erhebung von Daten zu Vermögensverhältnissen bei einer Depot-Eröffnung

Daten über die Vermögensverhältnisse von Wertpapierdepotkunden dürfen nur per Pflichtfeld erhoben werden, sofern die Erhebung der Daten für die Durchführung des Vertragsverhältnisses erforderlich ist.

Über eine Eingabe wurde ich auf eine rechtswidrige Datenerhebungspraxis einer Bank im Zusammenhang mit der Eröffnung eines Wertpapierdepots aufmerksam gemacht. Ein Bankkunde teilte mir mit, dass er bei einer Direktbank ein Wertpapierdepot eröffnet habe. Er habe sich legitimieren müssen und im Anschluss die Zugangsdaten für die Aktivierung des Depots erhalten. Um jedoch das Depot anschließend nutzen zu können, musste der Kunde Daten zu seinen Vermögensverhältnissen eingeben. Eine Möglichkeit, diesen Prozess zu umgehen und das Depot ohne Eingabe dieser Daten zu nutzen, bestand nicht.

Dieses Verfahren war datenschutzrechtlich unzulässig. Die Erhebung von personenbezogenen Daten ist zulässig, wenn die betroffene Person hierzu einwilligt oder die Erhebung auf eine Rechtsnorm gestützt werden kann (§ 4 Abs. 1 BDSG).

§ 4 Abs. 1BDSG

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

Eine Erhebung auf Grundlage eine Einwilligung war vorliegend nicht gegeben, da die Erhebung per Pflichtfeld erfolgte. Datenschutzrechtlich ist eine Einwilligung nur dann wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (§ 4a Abs. 1 BDSG). Von einer freien Entscheidung ist bei der Erhebung von Daten über Pflichtfelder hingegen nicht auszugehen.

Das Unternehmen stützte daher die Erhebung auf Regelungen aus dem Geldwäschegesetz (GwG) sowie dem Kreditwesengesetz (KWG). So sei die Überwachung der Geschäftsbeziehung durch die Direktbank auf unregelmäßige Transaktionen hin zu überprüfen. Um beurteilen

zu können, ob eine Transaktion auffällig ist, sei es erforderlich, die Informationen über die Einkünfte und des Vermögens der Betroffenen vorliegen zu haben.

Diese Auffassung wurde von mir nicht geteilt. So ist zwar das Unternehmen verpflichtet, Transaktionen daraufhin zu überprüfen, ob die auffällig sind. Dieses bezieht sich aber auf die Transaktion an sich, nicht aber auf die Transaktion in Bezug auf die Einkommens- oder Vermögensverhältnisse der Betroffenen.

Die Bank hat daraufhin den Prozess der Depoteröffnung in der Form neugestaltet, dass keine Daten zu Vermögenswerten mehr erhoben und die bereits erhobenen Daten gelöscht werden.

13.2
Anfertigung von Personalausweiskopien durch Banken

Banken sind nun dazu berechtigt und verpflichtet, unter bestimmten Voraussetzungen vollständige Kopien von Personalausweisen oder anderen Legitimationspapieren anzufertigen.

Das Kopieren von Ausweisen durch Banken ist immer wieder Gegenstand von Beschwerden. Mit Änderung des Geldwäschegesetzes (GwG) vom 23.06.2017 sind Banken neue Pflichten bezüglich der Aufzeichnung und Aufbewahrung von Legitimationspapieren auferlegt worden.

So sind Banken grundsätzlich verpflichtet, ihre Vertragspartner im Rahmen der Sorgfaltspflichten (§ 10 Abs. 1 Nr. 1 GwG) zu identifizieren. Die Identifikationsprüfung kann hierbei bei natürlichen Personen u. a. anhand eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, erfolgen (§ 12 Abs. 1 Nr. 1 GwG).

§ 10 Abs. 1 Nr. 1 GwG

Die allgemeinen Sorgfaltspflichten sind:

1. die Identifizierung des Vertragspartners und gegebenenfalls der für ihn auftretenden Person nach Maßgabe des § 11 Absatz 4 und des § 12 Absatz 1 und 2 sowie die Prüfung, ob die für den Vertragspartner auftretende Person hierzu berechtigt ist,

§ 12 Abs. 1 Nr. 1 GwG

Die Identitätsüberprüfung hat in den Fällen des § 10 Absatz 1 Nummer 1 bei natürlichen Personen zu erfolgen anhand

1. eines gültigen amtlichen Ausweises, der ein Lichtbild des Inhabers enthält und mit dem die Pass- und Ausweispflicht im Inland erfüllt wird, insbesondere anhand eines inländischen oder nach ausländerrechtlichen Bestimmungen anerkannten oder zugelassenen Passes, Personalausweises oder Pass- oder Ausweisersatzes

Die Bank als Verpflichtete im Sinne dieses Gesetzes muss die zu diesen Zwecken erhobenen Angaben aufzeichnen und aufbewahren (§ 8 Abs. 1 Nr. 1a GwG). Soweit die Identität des Vertragspartners beispielsweise durch Vorlage eines Personalausweises überprüft worden ist, muss nun eine vollständige Kopie dieses Dokumentes angefertigt werden (§ 8 Abs. 2 Satz 2 GwG). Diese ist fünf Jahre aufzubewahren und nach Ablauf dieser Frist unverzüglich zu vernichten (§ 8 Abs. 4 Satz 1 GWG). Sofern die Daten bei der Begründung einer Geschäftsbeziehung erhoben worden sind, beginnt die Fünf-Jahresfrist mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung beendet wird (§ 8 Abs. 4 Satz 2 GWG), in allen anderen Fällen mit dem Schluss des Kalenderjahres, in dem die jeweilige Angabe festgestellt worden ist.

§ 8 GwG

(1) Vom Verpflichteten aufzuzeichnen und aufzubewahren sind

1. die im Rahmen der Erfüllung der Sorgfaltspflichten erhobenen Angaben und eingeholten Informationen
   a) über Vertragspartner, gegebenenfalls über die für die Vertragspartner auftretenden Personen und wirtschaftlich Berechtigten,

...

(2) … Soweit zur Überprüfung der Identität einer natürlichen Person Dokumente nach § 12 Absatz 1 Satz 1 Nummer 1 oder 4 vorgelegt oder zur Überprüfung der Identität einer juristischen Person Unterlagen nach § 12 Absatz 2 vorgelegt oder soweit Dokumente, die aufgrund einer Rechtsverordnung nach § 12 Absatz 3 bestimmt sind, vorgelegt oder herangezogen werden, haben die Verpflichteten das Recht und die Pflicht, vollständige Kopien dieser Dokumente oder Unterlagen anzufertigen oder sie vollständig optisch digitalisiert zu erfassen. ...

(3) …

(4) Die Aufzeichnungen und sonstige Belege nach den Absätzen 1 bis 3 sind fünf Jahre aufzubewahren und danach unverzüglich zu vernichten. Andere gesetzliche Bestimmungen über Aufzeichnungs- und Aufbewahrungspflichten bleiben hiervon unberührt. Die Aufbewahrungsfrist im Fall des § 10 Absatz 3 Satz 1 Nummer 1 beginnt mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet. In den übrigen Fällen beginnt sie mit dem Schluss des Kalenderjahres, in dem die jeweilige Angabe festgestellt worden ist.

Damit kann die bislang vorherrschende datenschutzrechtliche Auffassung, eine Kopie des Personalausweises dürfe ausschließlich mit Einwilligung der betroffenen Person unter Hinweis auf die Möglichkeit der Schwärzung nicht benötigter Daten (Augenfarbe, Körpergröße etc.) erfolgen, nicht weiter aufrechterhalten werden. Mithin darf die/der Betroffene in vorgenannten Fällen nun die Anfertigung einer Ausweiskopie durch die Bank nicht mehr verweigern.

§ 10 Abs. 3 Nr. 1 GwG

Die allgemeinen Sorgfaltspflichten sind von Verpflichteten zu erfüllen;
1. bei der Begründung einer Geschäftsbeziehung,
…

13.3
Benachrichtigung über Datenübermittlung nach § 33 Abs. 1 Satz 2 BDSG

Unternehmen, die personenbezogene Daten ohne Kenntnis der betroffenen Person geschäftsmäßig speichern und diese erstmals übermitteln, sind dazu verpflichtet, die Betroffenen über die Tatsache der Übermittlung sowie die Art der übermittelten Daten zu informieren.

In großer Anzahl erreichen mich jedes Jahr Anfragen besorgter Bürgerinnen und Bürger, die von einer Auskunftei ein Schreiben erhalten haben, dass durch den Absender erstmals Anschriftendaten der Betroffenen erhoben und an Dritte übermittelt worden seien. Viele Betroffene sind, da sie weder zu dem Unternehmen eine Geschäftsbeziehung unterhalten oder dieses kennen, unsicher, warum Daten zu ihrer Person gespeichert und übermittelt worden sind.

Mit diesen Schreiben kommt die verantwortliche Stelle allerdings lediglich Pflichten nach, die ihr vom Gesetzgeber nach § 33 Abs. 1 Satz 2 BDSG auferlegt sind.

§ 33 Abs. 1 Satz 2 BDSG

Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Weiterführende Auskunft muss das Unternehmen nach dieser Rechtsnorm zunächst nicht erteilen. Hierfür besteht ein Auskunftsanspruch nach § 34 BDSG, welchen die Betroffenen gegenüber der verantwortlichen Stelle geltend machen können. Nach § 34 BDSG ist das Unternehmen verpflichtet, Auskunft zu erteilen über die gespeicherten Daten, den Zweck der Speicherung, die Herkunft der Daten und den Empfänger bei deren Weitergabe. Sofern es sich um fehlerhafte Daten handelt, kann sich ein Anspruch auf Berichtigung, Löschung oder Sperrung der Daten nach § 35 BDSG ergeben.

Eine Zustimmung zur Datenspeicherung ist bei den von Auskunfteien gespeicherten Daten nicht notwendig, wenn die Daten aus allgemein zugänglichen Quellen (z. B. öffentliche Register oder dem Internet) stammen (§ 29 Abs. 1 Nr. 2 BDSG).

§ 29 Abs. 1 Nr. 2 BDSG

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

…

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder ...

Ich empfehle den Betroffenen in diesem Zusammenhang, zunächst ihren Auskunftsanspruch nach § 34 BDSG gegenüber dem Unternehmen geltend zu machen und sodann anhand der Auskunft die gespeicherten Daten einer Prüfung zu unterziehen.

In keinem Beschwerdefall konnte bislang eine unzulässige Datenspeicherung und -übermittlung festgestellt werden.

13.4
SCHUFA Holding AG

Aufgrund ihrer hervorgehobenen Stellung im Bereich der Handelsauskunfteien bildet die Kontrolle der SCHUFA Holding AG (SCHUFA) in jedem Jahr einen Schwerpunkt meiner Tätigkeit. Betroffene erleiden durch negative Bonitätsauskünfte erhebliche Beeinträchtigungen, die dann in der Folge zu einer großen Anzahl von Beschwerden führen. Bei Verstößen gegen datenschutzrechtliche Vorschriften durch die SCHUFA handelt es sich jedoch angesichts des Umfangs an verarbeiteten Daten um Einzelfälle. Mehrere Eingaben betrafen Zuordnungsfehler von Datensätzen.

Mich erreichten mehrere Beschwerden über die fehlerhafte Zuordnung von gespeicherten Bonitätsinformationen zu betroffenen Personen. In allen Fällen waren negative Bonitätsinformationen falschen Personen zugeordnet worden. Die Bonität der betroffenen Personen wurde dadurch fälschlich negativ bewertet. Dies wirkte sich auf deren Möglichkeiten zum Abschluss von Geschäften aus.

Bei der Aufklärung der Ursachen wurde deutlich, dass die fehlerhaften Zuordnungen durch manuelle Bearbeitungen entstanden sind. Daher bat ich die SCHUFA um eine detaillierte Vorstellung der manuellen Bearbeitungshinweise.

Die Prüfung der manuellen Bearbeitungshinweise ergab hohe Hürden für die manuelle Zuordnung von Bonitätsinformationen durch Mitarbeiter der SCHUFA. Zusätzlich werden Mitarbeiter durch eine technische Auswertung der Treffergüte unterstützt, die keine Mängel erkennen ließ. Eine interne Auswertung der SCHUFA ergab zusätzlich das Vorliegen nur weniger Beschwerden über fehlerhafte manuelle Zuordnungen bei der SCHUFA.

Dennoch habe ich die SCHUFA darauf hingewiesen, dass eine fehlerhafte Zuordnung von Bonitätsinformationen trotz aller Bearbeitungssorgfalt nicht zu tolerieren ist. Jede fehlerhafte Auskunft kann bei betroffenen Personen zu erheblichen wirtschaftlichen Nachteilen führen. Daher sind Beschwerden über fehlerhafte Zuordnung bevorzugt und beschleunigt zu bearbeiten. Dies führte zu Ergänzungen in den Arbeitsanweisungen der SCHUFA.

13.5
Datenübermittlung von Versicherungsunternehmen an die Sozialverwaltung

Die Sozialverwaltung benötigt insbesondere im Bereich Sozialhilfe und der Grundsicherung für Arbeitsuchende („Hartz IV“) mitunter Informationen von Versicherern. Für solche Informationen (etwa über den Rückkaufswert einer Lebensversicherung des Betroffenen) gibt es gesetzliche Grundlagen, so dass es nicht auf eine Einwilligung des Betroffenen in die Datenübermittlung des Versicherers an die Sozialbehörde ankommt.

Der Anlass

Ein Versicherungsunternehmen ersuchte um Beratung, ob es zulässig ist, vermögensrelevante Daten von Versicherungskunden auf Ersuchen der Sozialverwaltung an diese zu übermitteln, oder ob in diesem Fall gar strafbares Handeln vorliegen könnte.

Rechtliche Bewertung

Die Bedenken wegen möglicher Strafbarkeit haben ihren Ursprung in § 203 StGB, der die Verletzung von Privatgeheimnissen u. a. durch Beschäftigte der Versicherer betrifft.

§ 203 Abs. 1 StGB

Wer unbefugt ein fremdes Geheimnis ... offenbart, das ihm als ...
...
6. Angehörigen eines Unternehmens der privaten Kranken-, Unfall oder Lebensversicherung...anvertraut worden oder sonst bekannt geworden, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Im vorliegenden Kontext, also Datenübermittlung an die Sozialverwaltung, ist der Rechtsbegriff „unbefugt“ in dieser Vorschrift der entscheidende Aspekt. Unbefugt handelt nämlich derjenige nicht, der zu diesem Handeln durch anderweitige Rechtsnormen berechtigt oder gar verpflichtet ist.

Dieses Hinzutreten von datenschutzrechtlich relevanten Normen wird im Bundesdatenschutzgesetz auch ausdrücklich angesprochen, wenn es dort heißt, dass die Erhebung, Verarbeitung

und Nutzung personenbezogener Daten zulässig ist, soweit das Bundesdatenschutzgesetz oder „eine andere Rechtsvorschrift“ dies erlaubt oder anordnet (§ 4 Abs. 1 BDSG).

Solche Rechtsvorschriften finden sich denn auch im Sozialrecht. Beispielsweise ordnen – freilich recht abstrakt formuliert – § 60 SGB II im Bereich der Grundsicherung für Arbeitsuchende („Hartz IV“) und § 117 SGB XII im Bereich der Sozialhilfe solche Datenübermittlungen insbesondere von Kreditinstituten, aber eben auch etwa von Lebensversicherern an (näher hierzu etwa Voelzke in Hauck/Noftz, SGB II, § 60 Rdnr. 33; Schlette in Hauck/Noftz, SGB XII, § 117 Rdnr. 33).

§ 60 Abs. 2 SGB II

Wer jemandem, der eine Leistung nach diesem Buch beantragt hat oder bezieht, zu Leistungen verpflichtet ist ... oder wer für ihn ein Guthaben führt oder Vermögensgegenstände verwahrt, hat der Agentur für Arbeit auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen.

§ 117 Abs. 3 SGB XII enthält dieselbe Regelung für den Bereich Sozialhilfe.

Ich habe das Versicherungsunternehmen über diese Rechtslage informiert.

14. Vereine, Verbände

14.1
Versand umfangreicher personenbezogener Dokumente anlässlich einer Mitgliederversammlung

Die Mitgliederversammlung als oberstes Organ eines Vereins sowie die vergleichbaren Gremien juristischer Personen ordnen ihre Belange durch Beschlussfassung. Zu diesem Zweck können sie sich mit allen den Verein betreffenden Angelegenheiten befassen, somit auch mit Belangen einzelner Vereinsmitglieder. Einem Verein ist es aber nicht gestattet, zur Vorbereitung von Entscheidungen umfangreiche personenbezogene Daten über einzelne Vereinsmitglieder (in digitaler Form) an die Teilnehmer der Mitgliederversammlung zu versenden.

Ein landesweit tätiger Sportverband wandte sich mit der Frage an mich, ob es zulässig sei, äußerst umfangreiche Unterlagen zu einer einzelnen Person an alle potentiellen Teilnehmer der Mitgliederversammlung zu versenden.

Hintergrund dieses Anliegens war ein verbandsinternes Streitschlichtungsverfahren. Der Verband sieht in seiner Satzung ein mehrstufiges Schlichtungsverfahren für interne Streitigkeiten vor, das an gerichtliche Verfahren angelehnt ist. Dabei sollen innerverbandliche Streitigkeiten wie z. B. Sanktionen gegen einzelne Mitglieder in verschiedenen „Instanzen“ geklärt werden. Laut Satzung entscheidet als letzte Instanz die Mitgliederversammlung über einzelne Streitfragen. Dabei wird aus allen bei der Mitgliederversammlung anwesenden Personen ein Spruchkörper gebildet, der üblicherweise aus ca. 10 bis 20 Personen besteht und den jeweiligen Streit entscheidet.

Im konkreten Fall sollte auf der regulär stattfindenden Mitgliederversammlung über eine Sanktion gegen ein einzelnes Verbandsmitglied entschieden werden. Die Beteiligten hatten bereits alle anderen „Instanzen“ des verbandsinternen Streitschlichtungsverfahrens durchlaufen. Dabei war ein knapp 100 Seiten umfassendes Dokument mit Schriftsätzen, Beweisstücken und einzelnen Schreiben von und zu der betroffenen Person entstanden, dessen Inhalt mit einer Gerichtsakte vergleichbar ist. Obwohl einige Stellen und Namen darin geschwärzt wurden, war für alle Verbandsmitglieder erkennbar, um welche Personen es sich jeweils handelt.

Dieses Dokument sollte als Anlage zur Einladung per E-Mail an alle potenziellen Teilnehmer der Mitgliederversammlung verschickt werden. Zur Mitgliederversammlung des Verbandes

werden mehrere hundert Personen eingeladen, von denen jedoch nur ein Teil tatsächlich auch an der Versammlung teilnimmt.

Der Versand derart umfangreicher personenbezogener Unterlagen an einen sehr großen Empfängerkreis ist jedoch unverhältnismäßig und datenschutzrechtlich unzulässig. Letztlich werden die Dokumente, wenn überhaupt, nur von wenigen Personen benötigt, die bei der Mitgliederversammlung den Spruchkörper bilden. Die Verbreitung an einen weit darüberhinausgehenden Personenkreis ist nicht erforderlich und gefährdet das Persönlichkeitsrecht der Beteiligten in unverhältnismäßigem Maße.

Der geplante Versand der Unterlagen wurde daher gestoppt und dem Verband wurde nahegelegt, seine internen Strukturen und Prozesse so zu ändern, dass entsprechend umfangreiche, personenbezogene Unterlagen nicht an einen derart großen Empfängerkreis versendet werden.

Daraufhin wurde vom Verband eine entsprechende Satzungsänderung angestoßen. Um den Personen, die z. B. als Mitglied eines Spruchkörpers tatsächlich Kenntnis der Unterlagen benötigen, die Einsicht in diese dennoch zu ermöglichen, ist nun die Hinterlegung der Unterlagen in körperlicher Form an einer zentralen Stelle vorgesehen. Die Personen, die berechtigterweise Einsicht nehmen, werden durch das Unterzeichnen einer Verschwiegenheitserklärung dazu angehalten, die darin enthaltenen Informationen nicht weiter zu verbreiten.

15. Verkehrswesen, Vermessung

15.1
Änderungen der Nutzungsbedingungen der DB-Lounges

Durch das Einscannen der BahnCard oder des Bahntickets 1. Klasse beim Zugang zu der DB-Lounge werden keine personenbezogenen Daten erhoben.

DB-Lounges sind Aufenthaltsräume an ausgewählten Bahnhöfen, in denen Reisende der 1. Klasse oder bahn.bonus comfort-Kunden sowie eine Person in ihrer Begleitung die Möglichkeit haben, ihre Wartezeit zwischen den Zugverbindungen bei einem kostenfreien Imbiss zu verkürzen. Hierbei stehen den DB-Lounge-Besuchern auch die T-Mobile Hot-Spots gratis zur Verfügung. Die DB-Lounges werden von der DB Fernverkehr AG betrieben.

Die Zutrittskontrolle wurde früher von den Mitarbeitern der DB-Lounge durchgeführt. Man musste die BahnCard oder das Ticket der 1. Klasse vorzeigen und der Zutritt wurde gewährt. Nach der Änderung der DB-Lounge Nutzungsbedingungen müssen die DB-Lounge Besucher die BahnCard oder das entsprechende Bahnticket einscannen, um Zutritt zur DB-Lounge zu erhalten. Eine Sichtkontrolle durch die Mitarbeiter findet nicht mehr statt.

Veranlasst durch die geänderte Verfahrensweise der DB-Lounge Nutzung erreichte mich eine Vielzahl von Eingaben betroffener Bahnkunden, die befürchten, dass durch die Betreiberin der DB Lounges Bewegungsprofile erstellt werden könnten. Ich habe mich mit dem Konzerndatenschutz der Deutschen Bahn in Verbindung gesetzt und die Auskunft bekommen, dass beim automatisierten Scan-Vorgang folgende Daten erhoben und gespeichert werden, unabhängig davon, ob es sich um eine BahnCard oder ein Bahnticket handelt:

– Zutrittsdatum,
– Legitimationsberechtigung (BahnCard oder Ticket),
– Klasse.

Beim Einscannen von Tickets werden zusätzlich erhoben und gespeichert:
– Tarif (Flexpreis, Sparpreis etc.),
– Start- und Zielbahnhof,
– Anzahl der Personen.

Beim Einscannen von BahnCards werden zusätzlich erhoben und gespeichert:

– BahnCard-Typ (BahnCard 25/50/100),
– Comfort-Status.

Zur Kontrolle der Gültigkeit wird nur das gültig von-/gültig bis-Datum geprüft, aber nicht gespeichert.

Die automatisierte Erfassung dient der Zutrittskontrolle und der statistischen Auswertung zum Zwecke der Verbesserung der Serviceleistungen und zum Zwecke der Steuerung der Auslastung. Bislang wurden diese Informationen manuell mittels Strichliste erhoben, was zu gewissen Unschärfen geführt hat. Um diese Unschärfen zu verringern und die Auslastung und den Service in den Lounges besser zu steuern, wird der Scanner eingesetzt.

Die Zählung der anonymisierten Daten per Scanner hilft daher, die Besucherzahlen und Kundengruppen in den verschiedenen Bereichen realistischer und zuverlässiger abzubilden. Gerade da die Zahl der Reisenden und somit potentieller Nutzer der Lounges zuletzt stetig gestiegen sind. Gleichzeitig wird mit der zeitgenauen Aufnahme der Besuchereingänge die Auslastung der Lounges sichtbar.

Die datenschutzrechtlichen Vorschriften finden erst dann Anwendung, wenn personenbezogene oder personenbeziehbare Daten verarbeitet werden. Personenbezogen oder personenbeziehbar sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG).

Beim Auswerten der erhobenen Daten wurde von mir festgestellt, dass keine Möglichkeit besteht, anhand der vorliegenden Daten Rückschlüsse auf einen bestimmten Kunden zu ziehen.

Auch für den Fall, dass gegenwärtig keine personenbezogenen Daten erfasst werden, haben die Bahnkunden die Befürchtung geäußert, dass die DB Fernverkehr AG ohne ihre Kenntnis die Datenverarbeitung so ausweiten könnte, dass die Erstellung von Bewegungsprofilen möglich wird. Mir wurde seitens des Konzerndatenschutzes der Deutschen Bahn zugesichert, dass keine weiteren Daten erhoben und gespeichert werden und keine Absicht bestehen würde, zukünftig die Datenspeicherung zu erweitern. Außerdem ergibt sich aus der Kommunikation, dass der Betreiberin der DB-Lounges durchaus bewusst ist, dass die Ausweitung der Datenverarbeitung auf die Erhebung auch personenbezogener Daten einer Rechtsgrundlage – z. B der Einwilligung des Bahnkunden – bedarf und dass eine unbefugte Erhebung und Verarbeitung von personenbezogenen Daten eine Ordnungswidrigkeit darstellt. Diese kann mit einer

Geldbuße bis zu 300 000 EUR geahndet werden (§ 43 Abs. 2 Nr. 1, Abs. 2 BDSG). Insofern gehe ich davon aus, dass die DB Fernverkehr AG auch zukünftig die Datenverarbeitung gemäß den gesetzlichen Vorschriften gestaltet.

Die DB Fernverkehr AG hat ihre Mitarbeiterinnen und Mitarbeiter in den Lounges bezüglich des o.a. Verfahrens geschult. Sie hält des Weiteren in ihren Lounges, um etwaigen Kundenbedenken schon im Vorfeld durch eine Information der Funktionsweise des Scanners zu begegnen, entsprechendes Info-Material (z. B. Aufsteller oder Flyer) für die Kunden vor.

15.2
Kameras am Straßenrand

Die Videoüberwachung im fließenden Straßenverkehr kann durch verschiedene Stellen veranlasst sein und unter Einsatz unterschiedlicher Technik erfolgen. Danach kann es in bestimmten Konstellationen zur Unanwendbarkeit von datenschutzrechtlichen Regelungen kommen.

Im Berichtszeitraum wurde ich mehrfach von Bürgern, öffentlichen Stellen und der Presse zur Zulässigkeit der Nutzung von Videotechnik im fließenden Straßenverkehr gefragt. Dabei standen drei Konstellationen im Mittelpunkt.

Verkehrszählungen zur Ermittlung des Durchgangsverkehrs durch öffentliche Stellen

Die Verkehrserhebung oder Verkehrszählung ist die Ermittlung der Anzahl der Fahrzeuge, die einen Straßenabschnitt, eine Kreuzung oder einen anderen Verkehrsknotenpunkt in einem bestimmten Zeitraum durchfahren. In der Regel geht es um die Ermittlung des Durchgangsverkehrs durch Gemeinden oder Städte zwecks verkehrlicher Planung. Die Analyse der Verkehrssituation und Einschätzung des Verkehrsaufkommens sind ein wichtiger Schritt, um nachhaltige Verkehrsplanung zu gewährleisten.

Die Zeiten, in denen Rentner oder Studenten mit Bleistift und Papier oder einer Zähluhr an Kreuzungen Verkehrszählungen durchführen, dürften wohl mittlerweile die Ausnahme darstellen. Die Messungen erfolgen heutzutage unter anderem anhand videobasierter Technik.

a) Die Anwendbarkeit von datenschutzrechtlichen Vorschriften ist bei Verkehrszählungen mithilfe videobasierter Technik zu bejahen, wenn durch sie personenbezogenen Daten erhoben und verarbeitet werden. Der für die Datenverarbeitung durch öffentliche Stellen maßgebliche § 2 Abs. 1 HDSG regelt, dass personenbezogene Daten Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener) sind. Im Zusammenhang mit Videoüberwachung im fließenden Verkehr sind Gesichter von Fahrzeuginsassen sowie Fußgängern oder Kfz-Kennzeichen personenbezogen. Für die Kfz-Kennzeichen trifft § 45 Satz 2 des Straßenverkehrsgesetzes (StVG) eine explizite Regelung über den Personenbezug von amtlichen Kennzeichen.

   Die Verarbeitung von Daten mit Personenbezug kann durch unterschiedliche technische Möglichkeiten je nach lokalen Gegebenheiten vermieden werden.

   Zunächst ist an die Aufnahmen mit geringer Auflösung bzw. an die Defokussierung der Bildschärfe zu denken, so dass weder Personen noch Kfz-Kennzeichen erkennbar sind und auch durch andere Merkmale keine Zuordnung zu Personen möglich ist. Dann kann durch die Montage der Kameras an erhöhten Stellen die Aufnahme von Gesichtern und Kfz-Kennzeichen umgangen werden. Außerdem bietet die Verpixelung von Gesichtern der Passanten sowie der Fahrzeuginsassen und der Kfz-Kennzeichen innerhalb des Kamerasystems eine Möglichkeit, sich der Anwendung datenschutzrechtlicher Regelungen zu entziehen. Schließlich ist an den Einsatz der sogenannten Blendbalken zu denken, mit denen bestimmte Bereiche – beispielsweise Fußgängerwege – ausgeblendet werden können. Ist durch Verwendung der oben aufgeführten Techniken sichergestellt, dass personenbezogene Daten im Rahmen normaler Geschehensabläufe nicht verarbeitet werden, dann finden datenschutzrechtliche Vorschriften mangels Personenbezug keine Anwendung.

b) Werden bei der Verkehrszählung personenbezogene Daten verarbeitet, muss eine datenschutzrechtliche Erlaubnisnorm (Rechtsgrundlage) vorliegen. Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten für Planungszwecke durch eine öffentliche Stelle ist § 32 HDSG.

§ 32 HDSG

(1) Für Zwecke der öffentlichen Planung können personenbezogene Daten gesondert verarbeitet werden. Die Verarbeitung soll von der übrigen Verwaltung personell und organisatorisch getrennt erfolgen.

(2) Die zu Planungszwecken gespeicherten personenbezogenen Daten dürfen nicht für andere Verwaltungszwecke genutzt werden. Sobald es der Zweck der Planungsaufgabe erlaubt, sind die zu diesem Zweck verarbeiteten personenbezogenen Daten so zu verändern, dass sie sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen. Eine Übermittlung von Daten, aus denen Rückschlüsse auf Einzelpersonen gezogen werden können, ist unzulässig.

c) Meistens werden die Verkehrszählungen unter Beteiligung eines privaten Auftragnehmers durchgeführt. Dabei handelt es sich um spezialisierte Firmen im Bereich der Verkehrszählung und Verkehrsplanung. § 4 HDSG räumt einer öffentlichen Stelle die Möglichkeit ein, personenbezogene Daten im Auftrag, auch durch Private, erheben, verarbeiten und nutzen zu lassen. Danach muss eine Gemeinde oder eine Stadt den Auftragnehmer sorgfältig unter besonderer Berücksichtigung der Zuverlässigkeit und Eignung auswählen und mit diesem einen schriftlichen Auftragsdatenverarbeitungsvertrag abschließen. Im Vertrag sind der Gegenstand und der Umfang der Datenverarbeitung, die technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen (§ 4 Abs. 2 S. 2 HDSG). Der private Auftragnehmer bestätigt im Auftragsdatenverarbeitungsvertrag, dass die Bestimmungen dieses Hessischen Datenschutzgesetzes eingehalten werden und er sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft. Der Auftraggeber hat mich vor Abschluss des Vertrages über die geplante Beauftragung zu unterrichten.

Verkehrszählungen zur Ermittlung des Durchgangsverkehrs durch nicht öffentliche Stellen

Auch private Unternehmen haben ein Interesse – beispielsweise bei der Standortplanung von neuen Filialen – den Durchfahrtsverkehr zu zählen. Auch in dieser Konstellation gilt, dass die datenschutzrechtlichen Regelungen keine Anwendung finden, wenn durch technische Maßnahmen sichergestellt wird, dass im Rahmen normaler Geschehensabläufe keine personenbezogenen Daten erhoben werden. Lässt sich die personenbezogene Verkehrserhebung nicht

vermeiden, benötigen auch die privaten Stellen nach § 4 Abs. 1 BDSG eine datenschutzrechtliche Erlaubnisnorm. Hier kommt § 28 Abs. 1 S. 1 Nr. 2 BDSG in Betracht. Diese Vorschrift gestattet die Verwendung der Daten im Rahmen einer Interessenabwägung zwischen den berechtigten Interessen der datenverarbeitenden Stelle und den schutzwürdigen Interessen des Betroffenen. Aufgrund der von der datenverarbeitenden Stelle durchzuführenden Interessenabwägung ist besonderes Augenmerk auf die Datenminimierung zu richten. Gleichermaßen bedienen sich viele private Unternehmen der Hilfe von spezialisierten Ingenieurbüros zur Erfassung des Durchgangsverkehrs. Auch hier muss der Auftragnehmer sorgfältig unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen ausgewählt und ein schriftlicher Auftragsdatenverarbeitungsvertrag abgeschlossen werden (§ 11 BDSG).

Tests von reparierten Geräten am Straßenrand

Die durch die Polizei für die Geschwindigkeitskontrolle benutzten Geräte werden teilweise von dem in Wiesbaden ansässigen Unternehmen VITRONIC repariert. Bei den anschließenden Funktionstests wird ein Testbild im öffentlichen Verkehr auf einer mit der Straßenverkehrsbehörde abgesprochenen Strecke angefertigt. Das Testbild wird von den Mitarbeitern begutachtet und anschließend – unabhängig von dem Prüfergebnis – unwiederbringlich sowohl auf den Testgeräten als auch im Backend gelöscht. Derartige Straßentests dienen der Vorbereitung des Eichtermins unter Laborbedienungen. Die Teststrecke wird mit einem Dreiecksständer „Testmessung“ am Straßenrand gekennzeichnet.

Dieses Testverfahren und die dabei stattfindende Datenverarbeitung von personenbezogenen Daten lässt sich ebenfalls auf § 28 Abs. 1 S. 1 Nr. 2 stützen. Denn die Erforderlichkeit der Gerätetests im Echtbetrieb im öffentlichen Verkehr folgt aus der Notwendigkeit der Funktionsauslösung unter realen Einsatzbedingungen. In Anbetracht der nur kurzzeitigen Speicherung der Testbilder und des nachvollziehbaren Interesses der Firma VITRONIC an den Straßentests fällt die in diesem Rahmen zu erfolgende Interessenabwägung zu Gunsten der datenverarbeitenden Stelle aus.

15.3
Beauftragung eines privaten Dienstleisters durch eine öffentliche Stelle

Eine öffentliche Stelle oder ein öffentlich-rechtliches Unternehmen kann ein privates Unternehmen mit der Verarbeitung personenbezogener Daten von Bürgern beauftragen, wenn ein wirksamer Auftragsdatenverarbeitungsvertrag abgeschlossen worden ist.

Im Berichtsraum habe ich mich mit Eingaben von Bürgern befasst, die im Zusammenhang mit der Erledigung von hoheitlichen Aufgaben von privaten Unternehmen kontaktiert wurden. Beispielhaft ist hier die Beauftragung eines privaten Unternehmens mit der Erfassung von Einwendungen im Rahmen eines Planfeststellungsverfahrens zu nennen. Auch gegen die Auslagerung von einzelnen Verarbeitungstätigkeiten durch ein öffentlich-rechtliches Unternehmen (öffentlich-rechtlicher Messstellenbetreiber) an einen Dienstleister (Techem) gab es Beschwerden. Die Bürger äußerten die Befürchtung, dass ihre personenbezogenen Daten den öffentlich-rechtlichen Bereich verlassen und privaten, weniger vertrauenswürdigen Dritten zur Verfügung gestellt werden würden. Es wurden Zweifel vorgetragen, ob ein solches Vorgehen mit datenschutzrechtlichen Grundsätzen vereinbar sei.

Das Rechtsinstitut der Auftragsdatenverarbeitung steht auch der öffentlichen Hand zur Verfügung.

Behörden und öffentlich-rechtliche Unternehmen

Für Behörden und öffentlich-rechtliche Unternehmen, die nicht am Wettbewerb teilnehmen, regelt § 4 HDSG die Übertragung von untergeordneten Hilfstätigkeiten auf dafür spezialisierte öffentliche oder private Auftragnehmer. Die übertragbaren, untergeordneten Hilfstätigkeiten haben nur den rein technischen Teil der Datenverarbeitung zum Gegenstand und erstrecken sich nicht auf das Verwaltungshandeln, dem die Daten dienen. Die hauptsächliche Verwaltungsaufgabe bleibt beim Auftraggeber, der als datenverarbeitende Stelle für deren rechtmäßige Erfüllung allein verantwortlich ist (§ 4 Abs. 1 S. 1 HDSG). Bei der Erledigung dieser Hilfstätigkeit ist der Auftragnehmer an Weisungen der öffentlich- rechtlichen Stelle strikt gebunden und hat keinen eigenen Beurteilungs- und Entscheidungsspielraum. Dies wird durch den zwischen dem Auftraggeber und Auftragnehmer schriftlich zu schließenden Auftragsdatenverarbeitungsvertrag sichergestellt. Der Mustertext eines solchen Auftragsdatenverarbeitungsvertrages steht auf meiner Internetseite (www.datenschutz.hessen.de) zur Verfügung.

Hat der Auftragnehmer bei der Verarbeitung von Daten einen Schaden verursacht, dann ist der Träger des Auftraggebers gegenüber dem Betroffenen zur Leistung von Schadensersatz nach § 20 HDSG verpflichtet. Somit steht im Falle des Schadensersatzes dem Bürger weiterhin ein solider Schuldner, die öffentliche Hand, gegenüber. Auch bezüglich anderer gesetzlicher Pflichten § 18 (Auskunft und Benachrichtigung) und § 19 (Berichtigung, Sperrung und Löschung) bleibt die öffentlich-rechtliche Stelle verpflichtet.

Der Auftragnehmer muss vom Auftraggeber sorgfältig ausgewählt werden (§ 4 Abs. 2 HDSG). Vor allem hat der Auftraggeber darauf zu achten, dass beim Auftragnehmer die erforderlichen Datensicherheitsmaßnahmen getroffen sind und muss ihre Einhaltung bei der Durchführung des Auftrags überprüfen.

Private Unternehmen fallen nicht in den Anwendungsbereich des HDSG, sondern unterliegen der Geltung des BDSG. Findet aber das HDSG auf den Auftragnehmer keine Anwendung, muss der öffentlich-rechtliche Auftraggeber gemäß § 4 Abs. 3 HDSG vertraglich sicherstellen, dass der Auftragnehmer die Bestimmungen des HDSG befolgt und sich der Kontrolle des Hessischen Datenschutzbeauftragten unterwirft.

Zusammenfassend lässt sich feststellen, dass den Bürgern durch das Rechtsinstitut der Auftragsdatenverarbeitung keine Nachteile entstehen. Die öffentlich-rechtliche Stelle bestimmt die Mittel und Zwecke der Datenverarbeitung, wählt den Auftragnehmer aus und überprüft die Einhaltung von vertraglichen Vereinbarungen. Die gesetzlichen Bestimmungen und die Aufsicht für die Datenverarbeitung bleiben so, als ob die Datenverarbeitung im öffentlichen Bereich verblieben wäre.

Öffentlich-rechtliche, am Wettbewerb teilnehmende Unternehmen

Für öffentlich-rechtliche, am Wettbewerb teilnehmende Unternehmen gelten über die Verweisnorm des § 3 Abs. 6 HDSG die Regelungen des Bundesdatenschutzgesetzes auch in Bezug auf die Auftragsdatenverarbeitung (§ 11 BDSG). Danach ist die Beauftragung eines privaten Dienstleisters durch ein öffentlich-rechtliches Wettbewerbsunternehmen zulässig. Auch in dieser Konstellation steht ein Mustertext für einen Auftragsdatenverarbeitungsvertrag auf meiner Internetseite zur Verfügung.

Weder die datenschutzrechtlichen Regelungen des HDSG noch die des BDSG verlangen eine Einwilligung oder eine Information an den Betroffenen über den Abschluss eines Auftragsdatenverarbeitungsvertrages.

15.4
Kennzeichnungspflicht für Drohnen

Seit 01.10.2017 besteht die Pflicht, die Drohnen mit dem Namen und der Adresse des Eigentümers zu versehen. Gegen diese Kennzeichnungspflicht bestehen keine datenschutzrechtlichen Bedenken.

Von der Kennzeichnungspflicht betroffene Eigentümer haben vorgetragen, dass durch die Kennzeichnungsverpflichtung personenbezogene Daten offenbart würden, ohne dass dafür eine Notwendigkeit bestehe. Den von den Eingebern an mich gerichteten Bitten, die durch die Drohen-Verordnung eingeführte Kennzeichnungspflicht wieder aufzuheben, konnte allein schon aus formellen Gründen nicht entsprochen werden. Die Normenkontrollkompetenz liegt bei den Gerichten. Allein die Gerichte haben die Befugnis, Rechtsnormen auf ihre Vereinbarkeit mit höherrangigem Recht zu überprüfen und die niederrangigen Normen im Falle der Nicht-Vereinbarkeit für nichtig zu erklären. Außerdem habe ich keine datenschutzrechtlichen Bedenken gegen die Einführung der Kennzeichnungspflicht.

Unter einer „Drohne“ versteht man ein unbemanntes Fluggerät. Die sogenannte Drohnen-Verordnung (Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten vom 30.03.2017) wurde vom Bundesministerium für Verkehr und digitale Infrastruktur erlassen und hat die Änderung von der Luftverkehrs-Zulassungs-Ordnung (LuftVZO) und die Änderung der Luftverkehrs-Ordnung (LuftVO) zum Gegenstand. Sie schreibt vor, dass Drohnen mit einer Startmasse von mehr als 0,25 Kilogramm an sichtbarer Stelle eine Kennzeichnung vorweisen müssen. Die Kennzeichnung muss dauerhaft fest mit dem Fluggerät verbunden und feuerfest sein. Die Verordnung ist seit dem 07.04.2017 in Kraft. Die Kennzeichnungspflicht gilt aufgrund einer Übergangsfrist seit 01.10.2017.

§ 19 Abs. 3 LuftVZO wurde wie folgt geändert:

Der Eigentümer eines Flugmodells oder eines unbemannten Luftfahrtsystems mit jeweils einer Startmasse von mehr als 0,25 Kilogramm, eines unbemannten Ballons oder Drachens mit jeweils einer Startmasse von mehr als 5 Kilogramm sowie eines Flugkörpers mit Eigenantrieb

muss vor dem erstmaligen Betrieb an sichtbarer Stelle seinen Namen und seine Anschrift in dauerhafter und feuerfester Beschriftung an dem Fluggerät anbringen.

Die die Kennzeichnungspflicht regelnde Luftverkehrs-Zulassungs-Ordnung ist eine Bundesverordnung und somit eine Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG. Diese Vorschrift bestimmt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig ist, soweit eine Rechtsvorschrift dies anordnet.

Der Verordnungsgeber verfolgte Zweck ist, die Haftungsprobleme für die Unfälle/Schäden zu lösen, die durch die Drohnen verursacht wurden. Zwar unterliegen unbemannte Luftfahrtsysteme und Flugmodelle bereits – wie alle Luftfahrzeuge – den Regelungen über die Halterhaftpflicht für Drittschäden nach den §§ 33 ff. LuftVG, die bei der Durchsetzung auftretenden Schwierigkeiten haben aber den Verordnungsgeber dazu veranlasst, die nun in § 19 Abs. 3 LuftVZO geregelte Kennzeichnungspflicht zur leichteren Bestimmung des Halters als den Haftungsverantwortlichen einzuführen.

§ 108 Abs. 1 Nr. 3 LuftVZO wurde wie folgt gefasst:

Ordnungswidrig im Sinne des § 58 Abs. 1 Nr. 10 des Luftverkehrsgesetzes handelt, wer vorsätzlich oder fahrlässig

…

3. entgegen § 19 Absatz 3 eine dort genannte Beschriftung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig anbringt,

…

Der Betrieb ohne entsprechende Kennzeichnung stellt eine Ordnungswidrigkeit gemäß § 108 Abs. 1 Nr. 3 LuftVZO dar. Die Ahndung der Ordnungswidrigkeiten liegt in der Zuständigkeit der Landesluftfahrtbehörden und nicht beim Hessischen Datenschutzbeauftragten.

16. Schwerpunkt Informationstechnik

16.1
Hessenbox: Cloud-Speicherlösung für hessische Hochschulen

Die Hessenbox ist eine Cloud-Speicherlösung, die den Austausch aller Formen von elektronischen Dokumenten an hessischen Hochschulen unterstützen soll. Die Cloud-Speicherlösung ist eine so genannte „private cloud“ ohne Archiv-Funktion, auch wenn einfache Recovery- und Backup-Strategien implementiert sind. Die Systemarchitektur ist geeignet für die Zwischenspeicherung von Dokumenten mit normalem Schutzbedarf.

Hessenbox als Speicherlösung „private cloud“

Der Wissenschaftsbetrieb basiert auf einem aktiven Informationsaustausch zwischen den Hochschulen bzw. deren wissenschaftlichen Personal. Zu diesem Zweck werden Cloud-Lösungen immer öfter nachgefragt. Bei der Nutzung von frei zugänglichen Cloud-Diensten, wie der Dropbox, ist in der Regel die Sicherheit und Nachvollziehbarkeit der Datenverarbeitung durch den Nutzer kaum zu durchblicken. Zudem muss der Betroffene einwilligen, dass der Cloud-Anbieter potentiell die abgelegten Dokumente nutzen kann. Soweit es dann um die Verarbeitung personenbezogener Daten geht, ist dies problematisch. Aber auch bei der Einstellung von z. B. Forschungsergebnissen in eine Cloud muss deren Sicherheit vor einem unbefugten Zugriff Dritter gewährleistet sein. Beides ist in hohem Maße im Interesse der Hochschulen.

Die Hessenbox ist aus dieser Perspektive eine echte Alternative, weil sie eine so genannte „private cloud“ ist. Der Zugang wird über eine zweckgebundene Auswahl von personenbezogenen Daten in geringer Anzahl aus den Identitätsmanagement-Systemen der jeweiligen Hochschulen gesteuert. Die Speicherung der elektronischen Dokumente verbleibt im Bereich der Hochschulen. Hierdurch liegt die vollständige Kontrolle bis auf die System- bzw. Hardwareebene ebenfalls bei den Hochschulen. Zudem unterliegt die Vergabe der Berechtigungen ausschließlich den Nutzenden, die die Rechte-Vergabe für ihre Verzeichnisse selbst verwalten. Detaillierte Informationen finden sich in der Beschreibung der Systemarchitektur einer heterogenen Infrastruktur.

Vertragliche Regelungen

Seit Juni 2016 besteht eine auf drei Jahre angelegte Anschubfinanzierung durch das Hessische Ministerium für Wissenschaft und Kunst (HMWK). Zunächst wurde die Kooperation zwischen der Justus-Liebig-Universität Gießen (JLU) und der Technischen Universität Darmstadt (TU DA) gestartet. Diese Kooperation sieht perspektivisch von Beginn an die Integration der Universitäten in Kassel und Frankfurt vor.

Seit Frühjahr 2017 sind die Verträge mit dem Ziel einer umfassenderen föderativen Struktur erweitert, so dass die hessischen Fachhochschulen in die Strukturen der Hessenbox als „private cloud"-Speicher integriert werden können.
Im Sachstandsbericht der Projekt-Verantwortlichen der JLU, TU DA und der Universität Kassel vom Dezember 2017 werden Aktivitäten der Johann Wolfgang Goethe-Universität und der Universität Kassel beschrieben sowie die Absicht der Philipps-Universität Marburg, sich an der Hessenbox zu beteiligen, genannt.

Schrittweiser Ausbau der Kooperationsstrukturen

Seit August 2016 begleite ich das Kooperationsprojekt, nachdem mir ordnungsgemäß die Auftragsdatenverarbeitung für die TU DA bei der JLU vorgelegt wurde. Gleichzeitig wurde eine Vorabkontrolle durchgeführt, so dass überarbeitete Verfahrensverzeichnisse vorliegen. Seit März 2017 läuft ein erster Pilotbetrieb in der Kooperation zwischen JLU und TU DA stabil.

Neben einem regen Austausch auf Dokumentenbasis fanden im Dezember 2016, im Februar 2017 und im Dezember 2017 kooperative Treffen mit den Projektteilnehmern bei mir im Haus statt. An diesen Treffen nahmen Projekt-Verantwortliche und Vertreter der JLU, der TU DA, der Universität Kassel und des HMWK teil. In der Sitzung im Dezember 2017 war der Datenschutzbeauftragte der Fachhochschule Darmstadt dabei, weil sich im Rahmen zukünftiger, föderativer Strukturen die Hochschulen insgesamt beteiligen wollen.

Zudem haben meine Mitarbeiter an Workshops zu föderalen Strukturen in Identitätsmanagement-Systemen der Hochschulen am Hochschulrechenzentrums (HRZ) der TU DA im Mai 2017 und im August 2017 an der Hochschule Darmstadt teilgenommen. Teilnehmende dieser Workshops waren, neben den Geschäftsleitungen der Rechenzentren, mehrheitlich die Beschäftigten in den technischen Abteilungen, die unterschiedliche Varianten konkreter technischer Lösungen diskutierten.

Außerdem war die Hessenbox ein Thema beim jährlichen Treffen der Hochschul-Datenschutzbeauftragten im November 2016 und Oktober 2017. Hier waren meine Mitarbeiter ebenfalls beteiligt.

Grundzüge in heterogenen Infrastrukturen

In Abhängigkeit von der Größe bzw. Studierendenzahlen, der daraus resultierenden notwendigen Zahl von Beschäftigten des wissenschaftlichen Stabs mit Forschenden in Festanstellung oder finanziert durch Drittmittelprojekte (oft als externer Personenkreis im Identitätsmanagement-System verwaltet) und der jeweiligen Verwaltung variieren die Anforderungen und Möglichkeiten der bestehenden IT. Dazu kommen in der Regel externe Kooperationspartner, die insbesondere in Projekte Zuarbeiten leisten.

Aus dieser Heterogenität der Finanzierungen und der Aufgaben ergeben sich unterschiedliche Strukturen in den Hochschulrechenzentren. Die Hochschulrechenzentren sind zunächst Dienstleister für ihre eigene Hochschule. Das jeweilige Rechenzentrum muss eine passende IT-Infrastruktur bereitstellen, so dass der Studienbetrieb vor Ort funktioniert. Dabei betreibt die heutige IT bereits für jede Hochschule und ihre Spezifika gesicherte Internet-Anbindungen, geschützte Web-basierte Applikationen und ggf. auch lokale Systeme.

Eine auf weitere Digitalisierung gerichtete, fortschreitende Entwicklung erfordert eine nochmalige Öffnung der Hochschulen bzw. der dazugehörigen Strukturen. Damit ist eine Anpassung der IT-Infrastrukturen erforderlich. Die betrachtete Cloud-Speicherlösung gehört zu den vorgenannten erforderlichen Verfahren und technischen Umsetzungen. Die Entwicklung erfährt eine datenschutzrechtliche, beratende Begleitung durch mein Haus.

Hinter der Cloud-Speicherlösung Hessenbox verbirgt sich eine Client-Server-Architektur, die der Heterogenität der bereits betriebenen IT-Systeme gerecht werden muss.

Die gesamte Software-Installation basiert auf dem PowerFolder-Produkt der Firma dal33t als einer so genannten Sync&Share-Lösung, die ggf. in verschiedenen Varianten genutzt werden kann.

Anlässlich des Kooperationsvertrags wurde insbesondere die implementierte Systemarchitektur zwischen der JLU und TU DA datenschutzrechtlich bewertet. Die Kooperation zwischen der JLU und der TU DA ist in folgender Weise ausgestaltet: Die Speicher liegen ausschließlich

im Rechenzentrum der JLU. Hier erfolgt eine nach einzelnen Hochschulen getrennte Verwaltung der Speicher und Zugriffssteuerung. Somit erfolgt kein direkter Zugriff auf Daten, die zur jeweiligen Universität gehören. Aus der Sicht der TU DA übernimmt die JLU eine Auftragsdatenverarbeitung. Der Vertrag zu Auftragsverarbeitung mit Vorabkontrolle wurde mir vorgelegt und geprüft.

Die Bedingungen für den Zugang und den Zugriff sind im Folgenden für die JLU-Box, wie auch die Hessenbox an der TU DA beschrieben.

Zugang

Die JLU realisiert einen Zugang, indem sie eine zweckgebundene Auswahl von personenbezogenen Daten – eine passende Teilidentität – auf ihre Echtheit prüft. Mit der eigenen Account-Verwaltung ist das einfach, da in diesem Fall das Hochschul-eigene Identitätsmanagement-System genutzt wird.

Die Anbindung der Teilidentitäten von Nutzenden der TU DA erfolgt durch die Übermittlung einer entsprechenden Teilidentität aus dem Identitätsmanagement-System der TU DA. Die Teilidentität besteht aus Kennung, Vor- und Nachname, E-Mail-Adresse und Datum des Tages der (letzten) Zustimmung zu den Nutzungsbedingungen für diesen Dienst. Das Passwort wird niemals aus dem (Ursprungs-) Identitätsmanagement-System übertragen, sondern im Anmeldeprozess gegen dieses im (Ursprungs-) Identitätsmanagement-System geprüft. Die Teilidentität wird nur übermittelt, wenn der oder die Beschäftigte der Nutzung zugestimmt hat. Die Zustimmung kann in Selbstverwaltung jederzeit widerrufen werden. Ein Löschprozess der gespeicherten Daten zur Person sowie der im Cloud-Speicher im Nutzerbereich abgelegten Daten wird initiiert. Nach dem Löschen besteht kein Anspruch auf die Wiederherstellung der Verzeichnisse und Dokumente, denn das System ist kein Archiv.

Zugriff

Die Zugriffsrechte werden durch die Nutzenden auf ihrer eigenen Verzeichnisstruktur vergeben. Der oder die Nutzende bestimmt, ab welchem Knoten im Verzeichnisbaum der Zugriff erfolgen darf. An die tiefer liegenden Verzeichnisstrukturen werden die Zugriffsrechte vererbt.

Generell wird zwischen einem „rein“ lesendem und änderndem Zugriff unterschieden. Wenn nur das Recht zum Lesen vergeben ist, dann können keine Änderungen und keine Löschungen vorgenommen werden. Das gilt sowohl für die Verzeichnisse als auch für die Dokumente. Wenn Änderungen erlaubt werden, dann ist es möglich, (Unter-)Strukturen anzulegen und zu löschen, wie auch Dokumente zu erstellen, zu speichern und zu ändern. Die Erlaubnis zu ändern beinhaltet auch das Löschen eines Dokuments. Das widerspricht datenschutzrechtlichen Grundsätzen eines differenzierten Berechtigungskonzepts.

Nur Beschäftigte der jeweiligen Hochschule haben eine festgelegte Quota, d. h. einen an sie zugewiesenem Festplattenspeicherplatz innerhalb des IT-Systems der Hessenbox. Damit haben auch nur sie die Möglichkeit, Berechtigungen zum Lesen und zum Ändern zu vergeben.

Beschäftigte können Studierende und andere externe Nutzerinnen und Nutzer einladen, wenn sie deren E-Mail-Adresse kennen. Nach der Einladung haben sich Studierende zu authentifizieren. Externe Nutzende müssen zuerst einen Account als „Gast“ beantragen, bevor sie ebenso die Applikation nutzen können. Solche Externen müssen mindestens den Nutzungsbedingungen des jeweiligen Rechenzentrums zustimmen. Wenn Studierende oder externe Nutzende in den Bearbeitungsprozess eingebunden werden sollen, dann geschieht das auf „Kosten“ der Quota des oder der jeweiligen Beschäftigten. Studierenden und externen Nutzenden wird aktuell keine Quota eingeräumt. Dementsprechend dürfen sie auch keine Rechte vergeben. Für Studierende ist jedoch eine Erweiterung geplant.

Zwei Varianten eines Clients

Es gibt zwei Varianten von Clients zur Nutzung der PowerFolder-Software. Zu unterscheiden sind der Web-Client, der für die jeweilige Hochschule „gebrandet“ ist und der aus einem App-Store heruntergeladen werden kann und der Zugriff über einen Web-Browser unter Verwendung der passenden URL.

In beiden Fällen haben die Nutzenden die Möglichkeit, direkt auf den Cloud-Speicher zuzugreifen, für den ihnen Nutzungsrechte eingeräumt wurden. Nach erfolgreicher Authentifikation und Autorisierung ist für eine Synchronisation für den zugeteilten Bereich zwischen Verzeichnis-Strukturen durchführbar. Der Web-Client aus dem AppStore gestattet nicht das Setzen und das Entziehen von Berechtigungen.

Eine Datenübertragung über ein mobiles Gerät funktioniert nur, wenn die Datenübertragung auf eigene Kosten angeschaltet ist. Die Datenübertragung ist in jedem Fall Transport-verschlüsselt. Die gespeicherten Dokumente liegen allerdings unverschlüsselt vor. Damit ergibt sich aus technischer Sicht die Bewertung, dass nur Daten ausgetauscht werden dürfen, die der Klassifizierung eines normalen Schutzbedarfs entsprechen.

Wenn einmal Verzeichnisstrukturen und die darin enthaltenen Dokumente heruntergeladen sind, obliegt es den Nutzenden, mit ihnen in datenschutzkonformer Weise zu verfahren.

Ausbau zur Föderation

Die PowerFolder-Lösung für den Zugang und den Zugriff auf die jeweiligen Bereiche von Cloud-Speichern erlauben auch das Einbinden weiterer Speicherstrukturen. Daher sind jetzt auch andere Hochschulen daran interessiert, sich diesem Verbund anzuschließen. Einige der bisherigen und zukünftigen Projektpartner sind mit mir im Gespräch und haben an den Treffen bereits teilgenommen.

Um die Zusammenarbeit in gleicher Weise gelingend voranzutreiben, ist zu empfehlen,
– die erarbeiteten Verträge,
– die überarbeitete Vorabkontrolle und
– das überarbeitete Verfahrensverzeichnis mit kleinen Anpassungen

als Muster für hessische Hochschulen zu nutzen. Das gilt insbesondere, wenn diese in der gleichen Weise eine anzuschließende Instanz des vorgestellten Cloud-Speichers nutzen möchten.

Datenschutzrechtliche Bewertung

Die Hessenbox selbst ist in ihrer jetzigen Umsetzung jeweils eine Einzellösung, für die keine datenschutzrechtlichen Bedenken bestehen.

Hinsichtlich der Verschlüsselung der Daten konnte bislang noch keine abschließende Lösung gefunden werden. Deshalb dürfen derzeit nur Daten mit normalem Schutzbedarf über diesen Cloud-Speicher der jeweiligen Hochschule ausgetauscht werden. Ferner wird empfohlen das vergleichsweise undifferenzierte Berechtigungskonzept zu verfeinern; insbesondere sollte

eine differenzierte Vergabe von Berechtigungen auf Operationsebene (erstellen, lesen, ändern, löschen) angestrebt werden. Idealerweise würde dies auch für einzelne Dokumente unterstützt werden.

Ich werde dieses wegweisende Projekt weiter datenschutzrechtlich begleiten und bei der Umsetzung der noch offenen Punkte beratend zur Verfügung stehen, insbesondere um eine datenschutzkonforme Erweiterung für föderative Strukturen mit weiteren Hochschulen zu gewährleisten.

16.2
Flächendeckende automatisierte Prüfungen von Web-Angeboten erforderlich

Die Einzelfallprüfung im Interesse eines Betroffenen stand bisher bei vielen Maßnahmen der Datenschutzbeauftragten im Vordergrund. Einige bei der Gestaltung von Web-Angeboten verwendete Techniken sind veraltet, rechtlich nicht (mehr) zulässig oder bis zu einer Entscheidung durch die Rechtsprechung zumindest umstritten. Ihre Verwendung kann nur durch automatisierte Prüfungen flächendeckend unterbunden werden.

Bestandsaufnahme von technischen Defiziten

Mehrfach hatte sich die IT-Abteilung im Jahr 2017 mit Eingaben zu beschäftigen, denen Pressemeldungen von technischen Defiziten insbesondere in Web-Applikationen vorausgegangen sind.

Als Reaktion auf derartige Eingaben erfolgen i. d. R. datenschutzrechtliche Prüfungen, in denen zu evaluieren ist,

– ob unbefugte Dritte Zugang zur Web-Applikation erhalten haben,
– ob ein unberechtigter Zugriff erfolgt ist oder
– ob in anderer Weise Datenabflüsse personenbezogener Daten stattgefunden haben.

Gemeinsame Interessen

Wenn mindestens einer dieser Punkte erfüllt ist, dann sind Vertraulichkeit und Integrität in Bezug auf die betroffenen personenbezogenen Daten ggf. nicht mehr gewährleistet. Ein unberechtigter Zugriff kann ferner genutzt werden, um die Verfügbarkeit zu beeinträchtigen. Die Belastbarkeit der Systeme kann mittels eines unbefugten Zugangs wie auch eines unberechtigten Zugriffs gestört werden. Offensichtlich ergeben sich gemeinsame Interessen, die sowohl im Bereich des Datenschutzes, der Datensicherheit als auch der IT-Sicherheit liegen.

Aus Sicht des Technischen Datenschutzes sind während einer datenschutzrechtlichen Prüfung alle ergriffenen Maßnahmen zu prüfen, die eine datenschutzkonforme Verarbeitung gewährleisten. Hier bestehen gemeinsame Interessen mit Absicherungen, die heute typischerweise im Bereich der IT-Sicherheit verortet werden.

Die Prüfpraxis aus technischer Sicht

Ein Beschwerdeführer oder auch ein Petent beklagt einen bestimmten – aus seiner Sicht rechtswidrigen – Umstand im Zusammenhang mit der Verarbeitung seiner personenbezogenen Daten. Im Regelfall der Auslöser für die Sachverhaltsfeststellungen durch die Datenschutzaufsichtsbehörden. Dies ist auch bei der Nutzung von Web-Angeboten nicht anders.

Dabei steht die Frage der Rechtmäßigkeit einer Datenverarbeitung zunächst im Vordergrund. Danach spielen auch immer wieder Fragen zur verwendeten Technik eine wesentliche Rolle. Die Aufsichtsbehörden machen sich dabei regelmäßig ein eigenes Bild von den Oberflächen eines Web-Angebotes. Hierzu prüfen sie die Einhaltung formaler Vorgaben (z. B. Impressum oder Datenschutzerklärung) und setzen sich im Folgenden je nach Fall auch mit den Fragen zu verwendeten Verschlüsselungstechniken, Tracking-Tools oder anderen technischen Fragen der Datenerhebung und -verarbeitung von Betroffenen auseinander.

Dabei werden alle Fakten gesammelt, die geeignet sind, die Daten verarbeitende Stelle sehr konkret zu einer Stellungnahme zum Sachverhalt aufzufordern bzw. gegen eindeutige Verstöße vorzugehen. In diesem Zusammenhang spielen die verwendeten Techniken zur Erfassung und Verarbeitung der Kundendaten eine zunehmende Rolle. Oft wird hier die Prüfung der Quelltexte eines Web-Angebotes notwendig. Da aus den Quelltexten aber nicht alle relevanten Fakten zweifelsfrei zu erkennen sind, wird immer häufiger eine zusätzliche Auswertung der Datenflüsse ins Internet unumgänglich.

Die hier beschriebene Einzelfallprüfung wird aber der Wirklichkeit der Web-Angebote im Internet nicht mehr gerecht. Dieses liegt u. a. darin begründet, dass bestimmte unzulässige Techniken regelmäßig im zumindest einstelligen Prozentbereich am Markt zu finden sind. Im Folgenden verdeutlichen einige bekannte Szenarien des vergangenen Jahres die Notwendigkeit solcher Prüfungen.

Beispielhafte Anlässe für flächendeckende Überprüfungen

Session-Replay

Ende des vergangenen Jahres wurde in verschiedenen Medien über die Ergebnisse von Forschern der Universität Princeton in den USA zum Thema „Session-Replay“ berichtet. Mit dieser Technik ist es möglich, insbesondere Benutzereingaben in Formularfeldern nachzuvollziehen und diese zur Auswertung des Benutzerverhaltens an einen Dienstleister zu übertragen. Davon werden aber auch Daten erfasst, die der Benutzer gar nicht abgeschickt hat, etwa weil er die Inhalte vorher nochmals überarbeitet hat. Darüber hinaus werden Daten mitübermittelt, die zunächst vom verwendeten Browser automatisiert in bekannte Felder eingesetzt und vom Benutzer danach aus individuellen Gründen abgeändert wurden.

Unabhängig davon, ob eine derartige Erfassung von Daten grundsätzlich rechtlich zulässig ist, dürfen diese Verfahren sicherlich nicht zum Einsatz kommen, wenn sie eine verschlüsselte Übertragung der Textfelder aushebeln und die Inhalte im Klartext an den Dienstleister zur Auswertung übermitteln.

Da die Forscher sich für ihre Untersuchung eine veröffentlichte Liste der weltweit meistbesuchten Web-Sites vorgenommen haben, wurden z. B. die deutschen „Ableger“ international arbeitender Konzerne nicht untersucht. Hier ergibt sich insgesamt der Anlass für eine jeweils eigene Untersuchung der Aufsichtsbehörden.

Facebook Custom Audience (FCA)

Bei dem seit einiger Zeit – je nach Umsetzung – rechtlich umstrittenen Einsatz von FCA werden die Daten der Webseiten-Benutzer an Facebook zur Auswertung des Surfverhaltens bzw. zur Optimierung des Angebots übermittelt. Die Verwendung dieses Tracking-Tools lässt sich

zum Teil im Quelltext der Seiten erkennen. Sie kann aber auch durch die verwendete Programmiertechnik verborgen bleiben und ist dann nur noch über die Prüfung der Datenflüsse zu den entsprechenden Servern im Internet nachzuweisen. Für eine individuelle Prüfung einer Seite lassen sich in diesem Fall auch verschiedene Browser-Ergänzungen verwenden, die FCA als eine von vielen verwendeter sogenannter Tracking-Techniken (engl.: tracking = verfolgen) unmittelbar anzeigen können.

Einsatz älterer SSL/TLS Zertifikate

Häufig werden von verschiedenen Seitenbetreibern mittlerweile veraltete und als unsicher eingestufte Verschlüsselungstechniken bzw. Zertifikate eingesetzt. Moderne Browser zeigen diese Problematik ggf. auch nur bei einer entsprechenden Voreinstellung unmittelbar mit dem Aufruf der jeweiligen Web-Seite an.

Unzureichende System-Konfigurationen

Immer wieder werden unbefugte Zugänge und Zugriffe gemeldet. Sie basieren oft auf Standard-Accounts, die z. B. für Tests in der Entwicklungsphase implementiert sind und nicht beim Go-Live entfernt werden. Konsequenterweise sind Verfahren der System-Härtung beim Übergang vom Softwareprojekt zum dauerhaften Betrieb einzusetzen, um Datenschutz-Vorfällen vorzubeugen. Das ist keine einmalige Aktivität, sondern erfordert ein kontinuierliches Verfahren, etwa auf der Basis eines IT-Sicherheits-Managementsystems (ISMS). Im Rahmen eines ISMS sind z. B. CERT-Meldungen zu betrachten und ggf. die entsprechenden (Gegen-)Maßnahmen zu ergreifen.

Konsequenzen

Wie die aufgeführten Fälle zeigen, ergibt sich für die Aufsichtsbehörden aus zum Teil sehr unterschiedlichen Anlässen ein Bedarf, weitgehend automatisiert auf Webseiten des eigenen Zuständigkeitsbereichs bestimmte Sachverhalte festzustellen.

Ich habe daher an einem der genannten Beispiele über 400 Web-Angebote aus Hessen in einer Stichprobe untersucht, um die Rahmenbedingungen und Erfordernisse für automatisierte Prüfungen zu analysieren. Für eine flächendeckende Betrachtung ist dabei die Erfassung aller

im Prüfzeitraum aus Hessen angebotenen Seiten notwendig. Da es dafür keinen online abrufbaren Katalog gibt, habe ich z. B. untersucht, ob eine Webseiten-Suche nach Impressum und einer Postleitzahl zu einer zutreffenden und für das weitere Vorgehen verwertbaren Liste führt. Für eine automatisierte Suche wäre dann der verfügbare Katalog aller hessischen Postleitzahlen einzusetzen. In weiteren Schritten sind die oben beschriebene Quelltextsuche, die Analyse der Verbindungsaufrufe oder weitere Methoden zur Feststellung bestimmter Sachverhalte zu automatisieren. Mit der kurzen Beschreibung kann nur angedeutet werden, wie sich die Prüfpraxis bei Web-Angeboten voraussichtlich weiterentwickeln wird. Die Aufsichtsbehörden werden einzelne Prüfungen ggf. auch als Aufträge an spezialisierte Firmen vergeben, sie müssen sich aber immer wieder neu mit der gerade verwendeten Technik und den anderen Parametern der Prüfaufträge auseinandersetzen.

Eine datenschutzrechtliche Prüfung von Web-Angeboten umfasst mehr als die technischen Realisierungen zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme. Im Grunde ist die Gesamtheit von zu ergreifenden Maßnahmen zu betrachten. Aus Sicht einer datenschutzrechtlichen Bewertung gehören dazu ebenso die organisatorischen Maßnahmen im jeweiligen Anwendungskontext.

17. Bilanz

17.1
„Schwarze Liste“ über Lehrer ist erneut ein Thema
(39. Tätigkeitsbericht, Ziff. 4.5.2)

Die „Informationsliste“ der Schulverwaltung zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte beschäftigte mich im Berichtszeitraum erneut. Bereits in meinem 39. Tätigkeitsbericht habe ich mich mit dem Thema auseinandergesetzt.

Der Erlass über die Informationsliste

Erlass vom 11.10.2012 (Az. IV.3-050.001.001 – 00143)

Bei der Zentralstelle Personalmanagement (ZMP) im Staatlichen Schulamt für die Stadt Darmstadt und den Landkreis Darmstadt-Dieburg wird eine „Informationsliste der Schulverwaltung zur Vermeidung der Wiedereinstellung ungeeigneter Lehrkräfte und für den Schuldienst ungeeigneter sozialpädagogischer Mitarbeiterinnen und Mitarbeiter“ geführt.

Die Informationssammlung verfolgt den Zweck, die im Bezirk eines Staatlichen Schulamtes gewonnene Information über die Nichteignung einer Person, zum Schutze der Schülerinnen und Schüler auch allen anderen Schulamtsbezirken zugänglich zu machen.
...

Nach meinen Ausführungen im 39. Tätigkeitsbericht (Ziff. 4.5.2), in dem ich über mangelnde Transparenz und verfahrensrechtliche Mängel berichtet hatte, wurden durch das Kultusministerium verbindliche Regelungen betreffend den Inhalt und die Nutzung der Liste in Form eines Erlasses geschaffen. Hierin wurden u.a. der Inhalt des Datensatzes über die betroffenen Personen sowie standardisierte Gründe für die Eintragung festgelegt.

Hinzu kam die Festlegung des zur Eintragung berechtigten Personenkreises sowie diejenigen, welche einen lesenden Zugriff auf die Daten haben. Die Schaffung einer Rechtsgrundlage im Nachgang meiner damaligen Prüfung war konsequent, ist jedoch verbesserungswürdig.

Vorgaben für die Löschung der Datensätze im Verfahrensverzeichnis

Keine Regelung enthält der Erlass hinsichtlich der Speicherfristen. Im Rahmen meiner Gespräche im Jahr 2009 wurde mir mitgeteilt, dass, wenn sich im Laufe der Zeit herausstelle, dass die Eignung nun vorhanden oder wiederhergestellt sei, die Löschung des Datensatzes des Betroffenen erfolge. Allerdings fehlen hierzu allgemeinverbindliche Regelungen. Erschwerend kommt in diesem Zusammenhang hinzu, dass jedes der Staatlichen Schulämter in Hessen in seinem Bezirk für die Einspeisung der Datensätze verantwortlich ist. In Darmstadt wird die Liste ausschließlich geführt und gepflegt. Allerdings wird der Mangel teilweise dadurch kompensiert, dass in jedem Staatlichen Schulamt ein Verfahrensverzeichnis erstellt wurde, in dem die Voraussetzungen für eine Löschung der Daten beschrieben sind. Anlass für eine Löschung kann dann z. B. die Nachholung einer benötigten Qualifikation sein oder die Verbesserung des Gesundheitszustandes, soweit derartige Gründe Anlass dafür waren, in die Liste aufgenommen zu werden.

Die Beschwerde eines Bewerbers, welcher in der Liste enthalten ist und die Löschung seiner Daten verlangte, zeigte die Problematik auf. Allerdings waren im konkreten Fall die Voraussetzungen für eine Löschung der Daten nicht gegeben.

Löschkonzept muss Bestandteil der Anwendung sein

Während in dem Erlass hinsichtlich der einzelnen Personenmerkmale sowie der Gründe für die Eintragung alles bis in Detail festgelegt und geregelt wurde, enthält dieser hinsichtlich der Speicherfristen keine Regelung. Hierzu teilte man mir 2009 mit, dass die Löschung des Datensatzes auf Betreiben der Betroffenen erfolge, wenn im Laufe der Zeit die Eignung (wieder)hergestellt sei. Das Defizit im Erlass hat man durch Hinweise im Verfahrensverzeichnis ausgeglichen.

Im Hinblick auf die Regelung in § 19 Abs. 3 HDSG, wonach Daten unverzüglich dann zu löschen sind, wenn diese zur weiteren Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich sind, ergibt sich hier eine Regelungslücke. Auch hinsichtlich der im Mai 2018 wirksam werdenden EU-Datenschutz-Grundverordnung (DS-GVO) und dem in Artikel 17 manifestierten „Recht auf Löschung“ ist es geboten, zu reagieren und Vorgaben für die Herausnahme, also Löschung von Datensätzen, zu machen.

In Gesprächen mit dem ZMP sowie dem Kultusministerium habe ich deutlich gemacht, dass die Novellierung des Erlasses deshalb absehbar erforderlich ist. Unabhängig hiervon ist das Verfahren durch verschiedene Gerichtsinstanzen bis hin zum Bundesverfassungsgericht überprüft und für zulässig erklärt worden.

17.2
Datenschutzrechtliche Aspekte bei der Führung von Schülerakten (45. Tätigkeitsbericht, Ziff. 3.4.2)

Im letztjährigen Tätigkeitsbericht habe ich grundsätzlich ausgeführt, was in eine Schülerakte aufzunehmen ist. Anlass für diesen Beitrag war u. a die Beschwerde von Eltern, welche die Aufnahme eines Fragebogens einer Psychologischen Ambulanz in die Akte des Sohnes kritisierten. Die Ambulanz hatte diesen Bogen mit Zustimmung der Eltern der Schule zum Ausfüllen übermittelt. Die zuständige Klassenlehrerin kopierte den ausgefüllten Bogen und führte diesen der Akte zu.

Neben der unzulässigen Speicherung von sensiblen, personenbezogenen Daten kam die Schulleitung meinem Auskunftsanspruch nicht nach. Auch die Einschaltung des Staatlichen Schulamtes (SSA) führte zunächst nicht weiter. Erst die Kontaktaufnahme mit dem Hessischen Kultusministeriums führte dazu, dass Schule und Schulamt meinem in § 29 HDSG normierten Anspruch Folge leisteten und Stellung bezogen.

Sowohl die Schule als auch das Schulamt waren der Ansicht, dass die Datenspeicherung zulässig war. Diese sei im schulischen Kontext erfolgt und deshalb von Relevanz. Außerdem sei es aus Gründen der Nachvollziehbarkeit des Verwaltungshandelns erforderlich gewesen, eine Kopie zu fertigen.

Ich habe daraufhin die Schule und das Staatliche Schulamt noch einmal die datenschutzrechtlichen Vorgaben bei der Führung von Schülerakten dargelegt. Die Datenspeicherung im Zusammenhang mit der Beantwortung des Fragebogens einer Psychologischen Ambulanz, der zur Beantwortung mit Zustimmung der Eltern an die Schule geschickt wurde, war unzulässig. Dies ergibt sich zum einen aus der Anlage 1 der Verordnung zur Verarbeitung personenbezogener Daten an Schulen. Dies ist ein abschließender Katalog, der eine Speicherung der in Rede stehenden Daten durch die Schule nicht vorsieht. Zum anderen obliegen die Daten einem Zweckbindungsgebot. Nach § 13 HDSG dürfen personenbezogene Daten grundsätzlich nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden

sind. Personenbezogene Daten in der öffentlichen Verwaltung dürfen nur zu einem bestimmten, rechtmäßigen Zweck erhoben oder gespeichert werden. Jede weitere Verarbeitung wird durch diesen Zweck begrenzt. Der Grundsatz der Zweckbindung dient somit auch der Transparenz des Verwaltungshandelns.

Die Psychologische Ambulanz hat mit Zustimmung der Eltern einen Fragebogen an die Schule übermittelt und um dessen Beantwortung gebeten. Die Schule hat den Bogen beantwortet und zurückübermittelt, zuvor jedoch eine Kopie angefertigt und der Schülerakte beigefügt. Damit wurde zum einen eine unzulässige Zweckänderung vorgenommen, zum anderen aber auch nicht der Versuch unternommen, die Eltern des betroffenen Schülers um die Erlaubnis hierfür zu bitten, denn eine Rechtsgrundlage für die Datenspeicherung gab es nicht. Im Gegenteil: ohne Wissen der Betroffenen wurde das Dokument, welches offensichtlich auch persönliche Einschätzungen der Klassenlehrerin enthielt, die den Schüler in ein ungünstiges Licht rückten, zum Bestandteil der Schülerakte.

In die Schülerakte gehören alle Unterlagen, die das Schulverhältnis der Schülerin oder der Schüler betreffen (§ 83 Abs. 1 S. 2 HSchG). Die Aufnahme der strittigen Informationen kann nicht hierunter subsumiert werden, da nicht der schulische Kontext im Vordergrund stand, sondern vorbereitende Aktivitäten der Psychologischen Ambulanz im Rahmen einer künftigen Behandlung des Schülers. Hierzu sollte die Schule Grundlagenwissen bereitstellen. Das Kultusministerium hat sich meiner Rechtsauffassung angeschlossen.

Ich gehe davon aus, dass sich die Schule künftig an die datenschutzrechtlichen Vorgaben hält. Die Eltern habe ich entsprechend in Kenntnis gesetzt.

17.3
Einsatz von Funkwasserzählern
(43. Tätigkeitsbericht, Ziff. 4.1.5.8; 45. Tätigkeitsbericht, Ziff. 4.4.3)

Die Eingaben zur Zulässigkeit der Einführung von Funkwasserzählern reißen nicht ab. Auch die Wasserversorgungsunternehmen – verunsichert durch die öffentlich geführten Diskussionen – wenden sich an mich mit Beratungsanfragen.

Ich habe mich in den vorhergehenden Tätigkeitsberichten mit dem Thema befasst und eine Möglichkeit aufgezeigt, wie die Einführung von funkbasierten Wasserzählern datenschutzkon-

form ausgestaltet werden kann. Im Kreise der Landesdatenschutzbeauftragten besteht weiterhin keine Einigkeit, ob für die Einführung der funkbasierten Messtechnik die Schaffung einer bereichsspezifischen, formell gesetzlichen Verarbeitungsgrundlage zu fordern ist oder ob §§ 18, 20, 24 der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser des Bundeswirtschaftsministeriums (AVBWasserV) auf der Grundlage von Art. 243 EGBGB eine ausreichende Verarbeitungsgrundlage darstellen. Ich habe in meinem 45. Tätigkeitsbericht die letztgenannte Ansicht vertreten und §§ 18, 20, 24 AVBWasserV in Verbindung mit der Anpassung der Wasserversorgungssatzung als datenschutzrechtliche Verarbeitungsgrundlage für ausreichend angesehen.

In den Beratungsanfragen der Wasserversorger wird häufig der Wunsch geäußert, dass ich das funkbasierte Verfahren prüfe und freigebe. Abgesehen von den fehlenden personellen Kapazitäten meiner Behörde wurde vom Landesgesetzgeber eine andere Verfahrensweise für die Feststellung der Datenschutzkonformität vorgesehen.

Die hessischen Wasserversorgungsunternehmen sind in der Regel öffentliche Unternehmen, die nicht am Wettbewerb teilnehmen und für die damit das Hessische Datenschutzgesetz gilt. § 6 Abs. 6 HDSG ordnet die Durchführung einer Vorabkontrolle durch den für das Verfahren zur automatisierten Datenverarbeitung Zuständigen an. Vor dem Einsatz eines solchen Verfahrens müssen die Gefahren für das Recht auf informationelle Selbstbestimmung untersucht und gefahrabwendende, technische und organisatorische Maßnahmen eingeführt werden. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zuzuleiten. Dieser kann sich nach Durchführung der Kontrolle des Verfahrens und bei Zweifeln an seiner Rechtmäßigkeit von mir beraten lassen.

17.4
Datenschutz bei Smart-TV-Diensten
(44. Tätigkeitsbericht, Ziff. 5.3)

Bei einer gemeinsam mit anderen Datenschutzaufsichtsbehörden durchgeführten Prüfung von Smart-TV-Geräten wurden verschiedene datenschutzrechtliche Defizite festgestellt. Die Gerätehersteller mit Sitz in Hessen haben inzwischen nachgebessert und ihre Smart-TV-Dienste transparenter und rechtskonform gestaltet.

Gemeinsam mit mehreren anderen deutschen Datenschutzaufsichtsbehörden habe ich vor einiger Zeit eine Prüfung von Smart-TV-Geräten durchgeführt, über die ich bereits im 44. Tätigkeitsbericht berichtet habe (Ziff. 5.3). Bei der Prüfung zeigten sich Defizite bei der Transparenz der Datenverarbeitung bei Smart-TV-Diensten und es wurden einzelne Datenverarbeitungsvorgänge ausgemacht, die in der praktizierten Form nicht zulässig waren.

Die Ergebnisse dieser Prüfung habe ich mit den in Hessen ansässigen Herstellern, deren Geräte geprüft wurden, ausführlich beraten und anschließend auf die Beseitigung der festgestellten Defizite hingewirkt.

Smart-TVs bieten den TV-Zuschauern diverse, zumeist von den jeweiligen Geräteherstellern angebotene Dienste, die über den reinen Fernsehkonsum hinausgehen und mittels einer Internetverbindung realisiert werden (z. B. Apps, Zugriff auf Mediatheken und Streaming-Dienste, HbbTV etc.). Mit der Nutzung solcher Internetdienste geht jedoch immer auch die Verarbeitung von Daten einher, die zum Teil auch Rückschlüsse auf bestimmte oder bestimmbare Personen zulassen. Vollständig anonymes Fernsehen ist mit einem Smart-TV daher letztlich nur möglich, wenn die Internetverbindung des Geräts gekappt bzw. gar nicht erst hergestellt wird. Dann kann mit dem Gerät, wie mit einem herkömmlichen Fernseher ohne Smart-TV-Funktionen, über Antenne, Satellit oder Kabelanschluss ferngesehen werden, ohne dass Daten des Zuschauers verarbeitet werden. In diesem Fall sind jedoch auch alle zusätzlichen Funktionen, die das Smart-TV-Gerät bietet, nicht nutzbar.

Werden die Smart-TV-Funktionen dagegen genutzt, entstehen rege Datenflüsse zwischen dem Fernseher und den jeweiligen Diensteanbietern. Viele dieser Datenflüsse, die bei der Geräteprüfung der Aufsichtsbehörden festgestellt wurden, sind allerdings erforderlich, um die jeweiligen Dienste überhaupt erbringen zu können. Die Verarbeitung von Daten zu diesem Zweck kann in aller Regel auf gesetzliche Rechtsgrundlagen gestützt werden und ist somit zulässig. Zudem haben die Nutzer meist den Geschäftsbedingungen, die für die jeweiligen Dienste gelten, ausdrücklich zugestimmt.

Soweit die Prüfungsergebnisse an einigen Stellen Verbesserungsbedarf hinsichtlich des Datenschutzes aufzeigten, sind die Hersteller auf die Forderungen und Anregungen meiner Behörde eingegangen und haben an verschiedenen Stellen ihre Dienste nachgebessert. So werden bestimmte Informationen zur Gerätenutzung nunmehr entweder gar nicht mehr erhoben oder zumindest nur noch in einer Weise, die keine Rückschlüsse auf einzelne TV-Nutzer mehr zulässt. Bei einem Hersteller wurden beispielsweise verschiedene geräteinterne IDs eingeführt, mittels derer ursprünglich gemeinsam gespeicherte Daten zum Gerät bzw. zum Nutzer

nunmehr getrennt werden. Auf diese Weise wird eine theoretisch mögliche Profilbildung zu den Vorlieben eines Nutzers deutlich erschwert. Zudem konnte erreicht werden, dass die Smart-TV-Nutzer inzwischen deutlich transparenter, umfangreicher und offener über Datenverarbeitungsvorgänge informiert werden und häufiger die Möglichkeit haben, diesen selbst zuzustimmen oder auch zu widersprechen.

Letztlich ist die Nutzung der komfortablen Funktionen von Smart-TV nicht möglich, ohne dass dabei Daten verarbeitet werden, die den Diensteanbietern teilweise auch Rückschlüsse auf die jeweiligen Nutzer erlauben. Wenn die Nutzer darüber jedoch zumindest hinreichend informiert werden, können sie selbst bestimmen, inwieweit sie die Verarbeitung ihrer Daten zugunsten der Nutzung bestimmter Dienste und Funktionen in Kauf nehmen wollen.

18. Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

18.1
Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 24.01.2017

Novellierung des Personalausweisgesetzes
Änderungen müssen bürger- und datenschutzfreundlich realisiert werden

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BRDrucks. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

– Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.

– An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eID-Funktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.

– Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

– Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.

– Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.

– Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.

– Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.

– Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

18.2
Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 15.03.2017

Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BRDrucks. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtsicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist. Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlautend ausgestaltet werden.

18.3
Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 17.03.2017

Kritik am Entwurf für ein neues BKA-Gesetz

Der vorgelegte Entwurf, mit dem die Rechtsprechung des BVerfG sowie die neue EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umgesetzt werden soll, beschneidet mit der Neustrukturierung der Datenverarbeitung durch die Polizei die Grundrechte. Hiergegen wendet sich die vorliegende Entschließung der DSK unter Enthaltung des Landes Sachsen.

Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BTDrucks. 18/11326 und 18/11163; BRDrucks. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungs-

gerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante "Mitziehautomatik" erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen "auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden" bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

18.4
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 29./30.03.2017

Göttinger Erklärung –
Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die

Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität“ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu

achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

18.5
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 29./30.03.2017

Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen "abweichendes Verhalten" erkannt werden soll.*

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken.

Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs, der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von Kfz-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von Kfz-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum

Abgleich der Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

* Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“.

18.6
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 08./09.11.2017

Keine anlasslose Vorratsspeicherung von Reisedaten

Der Gerichtshof der Europäischen Union (EuGH) hat in seinem Gutachten vom 26. Juli 2017 (Gutachten 1/15) zum Fluggastdaten-Abkommen der EU mit Kanada die langfristige Speicherung von Fluggastdaten (Passenger Name Records – PNR-Daten) sämtlicher Passagiere für nicht mit der Europäischen Grundrechtecharta vereinbar erklärt und seine Position zu anlasslosen Speicherungen personenbezogener Daten bekräftigt. Er erteilt damit einer anlasslosen Vorratsdatenspeicherung von personenbezogenen Daten erneut eine klare Absage. Die Aussagen des EuGH sind nicht nur auf alle geltenden PNR-Instrumente übertragbar und stellen Anforderungen an die Anpassung des Fluggastdatengesetzes, sie betreffen auch die auf europäischer Ebene angestrebte Einrichtung eines Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS), die ebenfalls weitreichende anlasslose Speicherungen beabsichtigen.

Zwar hält der EuGH es grundsätzlich für zulässig, Fluggastdaten automatisiert zu übermitteln und auszuwerten, um Personen zu ermitteln, die eine potentielle Gefahr für die öffentliche Sicherheit darstellen und bei ihrer Einreise einer gewissenhaften Kontrolle unterzogen werden sollen. Das gilt jedoch nicht für sensible Daten, die Rückschlüsse etwa auf die rassische und ethnische Herkunft, religiöse Überzeugungen oder das Sexualleben ermöglichen. Der Übermittlungszweck rechtfertigt auch nicht automatisch die weitere Verwendung und Speicherung der Daten. Die übermittelten Daten haben vielmehr ihren Zweck erfüllt, wenn sich während des Aufenthaltes keine konkreten Anhaltspunkte für geplante terroristische oder andere

schwere Straftaten ergeben haben. In diesem Fall sieht der EuGH keine Rechtfertigung für eine weitere Speicherung der Daten.

Das Fluggastdatengesetz, mit dem die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von PNR-Daten zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität umgesetzt wurde, geht insbesondere durch die Einbeziehung der innereuropäischen Flüge, die im Widerspruch zu dem Grundsatz des freien Personenverkehrs im Schengen-Raum steht, noch über den verpflichtenden Teil der Richtlinie hinaus.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sieht in den vom EuGH ausgesprochenen Feststellungen zur Rechtslage einen unverzichtbaren Maßstab für die Verordnungsvorschläge zur Einrichtung eines neuen Entry-Exit-Systems (EES) sowie eines EU-weiten Reiseinformations- und -genehmigungssystems (ETIAS).

Mit dem EES sollen alle Ein- und Ausreisen sowie Einreiseverweigerungen von Drittstaatlern in die EU zentral erfasst und für mehrere Jahre gespeichert werden (einschließlich biometrischer Identifizierungsmerkmale). Im ETIAS sollen zum Zwecke der Erleichterung der Grenzkontrollen vorab Daten von einreisewilligen visa-befreiten Drittstaatlern erhoben und ebenfalls für mehrere Jahre zentral gespeichert werden. In beiden Datenbanken sollen also Daten, die im Rahmen der Einreise und Grenzkontrolle erhoben werden, ebenso wie nach dem PNR-Abkommen, ohne konkreten Anlass zentral für einen langen Zeitraum vorgehalten werden. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hält dies nicht für vertretbar.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert die jeweils zuständigen Gesetzgeber auf, zeitnah und konsequent sämtliche PNR-Instrumente der EU im Sinne der EuGH-Rechtsprechung nachzubessern, insbesondere das deutsche Fluggastdatengesetz.

Sie fordert die Bundesregierung zudem auf, sich auf europäischer Ebene für eine den Anforderungen der EU-Grundrechtecharta und der Rechtsprechung des EuGH entsprechende Ausgestaltung der angestrebten Systeme EES und ETIAS einzusetzen.

18.7
Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 08./09.11.2017

Umsetzung der DS-GVO im Medienrecht

Das Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) und deren Geltungsbeginn im Mai 2018 verlangt eine Anpassung der medienrechtlichen Datenschutzbestimmungen an die neuen Vorgaben. Dabei muss dem hohen Stellenwert der Meinungs- und Informationsfreiheit sowie der Presse-, Rundfunk- und Medienfreiheit gemäß Art. 5 Grundgesetz (GG) und Art. 11 EU-Grundrechtecharta (GRCh) für die freiheitliche demokratische Grundordnung ebenso Rechnung getragen werden wie dem Recht auf Informationelle Selbstbestimmung gemäß Art. 1 i. V. m. Art. 2 GG und dem Recht auf Schutz personenbezogener Daten gemäß Art. 8 GRCh. Kollisionen der Schutzbereiche der Grundrechte sind im Sinne einer praktischen Konkordanz aufzulösen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist daher auf die Anpassungsklausel des Art. 85 DS-GVO hin. Danach können die Mitgliedstaaten Ausnahmen und Abweichungen von bestimmten Vorgaben der DS-GVO normieren, wenn „dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“. Das sich daraus ergebende Regel-Ausnahme-Verhältnis bedeutet, dass die Vorgaben der DS-GVO grundsätzlich auch auf sämtliche Verarbeitungen personenbezogener Daten zu grundrechtlich besonders geschützten journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken angewendet werden sollen.

Bei der Umsetzung von Art. 85 DS-GVO gilt es insbesondere folgende Anforderungen zu beachten:

– Ausnahmen oder Abweichungen von der Anwendung der DS-GVO auf die Verarbeitung personenbezogener Daten im journalistischen Bereich müssen notwendig sein, um freie Meinungsäußerung und Informationsfreiheit gemäß Art. 11 GRCh sicherzustellen.

– Einen regelhaften Vorrang der Presse-, Rundfunk- und Medienfreiheit sieht die DS-GVO nicht vor. Sie verlangt vielmehr, einen angemessenen Ausgleich zwischen den Grundrechten herzustellen, wenn diese in Widerstreit geraten (vgl. 153. Erwägungsgrund der DS-GVO).

– Die Grundsätze des Datenschutzes (Art. 5 DS-GVO) müssen hinreichend Beachtung finden. Jedenfalls steht es nicht im Einklang mit dem Recht auf Schutz personenbezogener Daten, wenn die Grundsätze des Datenschutzes im Journalismus in weitem Umfang ausgeschlossen werden. Eine Regelung kann keinesfalls als notwendig i. S. d. DS-GVO angesehen werden, wenn sie zum Zwecke der Abwägung mit der Meinungs- und Informationsfreiheit die Transparenzrechte und Interventionsmöglichkeiten für betroffene Personen sowie Verfahrensgarantien über eine unabhängige Aufsicht missachtet.

– Über den eingeräumten Gestaltungsspielraum geht es hinaus, wenn die Verarbeitung personenbezogener Daten durch Hilfsunternehmen zu undifferenziert vom Geltungsbereich der DS-GVO ausgenommen wird, ohne dass diese Aktivitäten unmittelbar der journalistischen Tätigkeit dienen. Die Reichweite der journalistischen Tätigkeit bedarf zudem einer Konkretisierung.

– Die künftige Aufsicht über den Datenschutz beim Rundfunk ist unabhängig auszugestalten. Sie bedarf wirksamer Abhilfebefugnisse bei Datenschutzverstößen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher für die Anpassung von Rundfunk-Staatsverträgen, Presse- und Mediengesetzen:

– Die gesetzlichen Anpassungen i. S. d. Art. 85 DS-GVO müssen konkret und spezifisch – bezogen auf die jeweiligen Normen und Vorgaben der DS-GVO – Ausnahmen und Abweichungen regeln und diese begründen.

– Bei der Ausübung der jeweiligen Regelungskompetenz ist das europäische Datenschutzrecht zwingend zu beachten. Eine faktische Beibehaltung der bisherigen nationalen Rechtslage würde dem nicht gerecht.

19. Materialien zur DS-GVO

Vorbemerkungen zu den Kurzpapieren Auslegungshilfen zum neuen Datenschutzrecht

Die Europäische Datenschutz-Grundverordnung (DS-GVO) wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden befassen sich zurzeit intensiv mit den neuen Rechtsgrundlagen und deren Anforderungen und stimmen eine einheitliche Sichtweise ab. Erste Ergebnisse dieses Prozesses sind gemeinsame Kurzpapiere zur DS-GVO, die die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ab sofort veröffentlicht (s. a. www.datenschutz.hessen.de).

Diese Kurzpapiere dienen als erste Orientierung, wie nach Auffassung der Datenschutzkonferenz die Datenschutz-Grundverordnung im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss.

19.1
Kurzpapier Nr. 1

Verzeichnis von Verarbeitungstätigkeiten – Art. 30 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.

Altes Recht = neues Recht?

Das aus dem BDSG bekannte Verfahrensverzeichnis (§ 4g Abs. 2 und 2a BDSG; dort „Übersicht“ genannt) wird mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte

Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und – neu – auch jeder Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet. Es wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verfahrensverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein.

Stellen mit weniger als 250 Mitarbeitern

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

– die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
– die nicht nur gelegentlich erfolgen (z. B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder
– die besonderen Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist. Da es anders als in Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) nicht darauf ankommt, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt, sondern jedes Risiko für die Rechte und Freiheiten bezüglich der Verarbeitung zu betrachten ist, wird vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten sein.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Anders als im bisherigen BDSG ist eine Möglichkeit für jedermann, in das Verzeichnis von Verarbeitungstätigkeiten Einsicht zu nehmen, nach der DS-GVO nicht vorgesehen. Ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Meldepflichten von manchen Unternehmen an die Aufsichtsbehörde. Erstellt und vorgehalten werden müssen die

Verzeichnisse dennoch, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung zu stellen sind (siehe Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Inhalt des Verzeichnisses für Verantwortliche (Art. 30 Abs. 1 DS-GVO)

Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DS-GVO wesentliche Angaben zur Verarbeitung beinhalten wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Verantwortliche Stellen, die bereits jetzt über ein strukturiertes Verfahrensverzeichnis oder eine strukturierte Datenschutzdokumentation zu den Verfahren verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine Probleme haben.

Inhalt des Verzeichnisses für Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

Ein Verzeichnis beim Auftragsverarbeiter zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung war vom BDSG bislang nicht vorgeschrieben. Nach Art. 30 Abs. 2 DS-GVO ist ein solches Verzeichnis jedoch künftig zu erstellen.

Auch hier sind die Pflichtangaben überschaubar, so dass der Aufwand, dieses Verzeichnis zu erstellen, als eher gering einzustufen sein wird.

Beschreibung technischer und organisatorischer Maßnahmen

Art. 30 Abs. 1 lit. g und Art. 30 Abs. 2 lit. d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

Rechtsfolgen bei Verstoß

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße sanktioniert werden.

Das Verzeichnis als Teil der Rechenschaftspflicht

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden.

Ausblick: Wesentliche Rolle des Verzeichnisses und Muster-Vorlage der Datenschutzaufsichtsbehörden

Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verfahrensverzeichnisse eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können.

Die deutschen Aufsichtsbehörden werden im Jahr 2017 eine Muster-Vorlage sowie weitere Hinweise für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO bereitstellen.

Unsere Empfehlung

Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Übergangszeit bis zur Geltung der DS-GVO

am 25.05.2018 sollte dazu genutzt werden, die bereits bestehende Verfahrensdokumentation an die neuen Anforderungen anzupassen.

19.2
Kurzpapier Nr. 2

Aufsichtsbefugnisse/Sanktionen

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 DS-GVO stellt den Aufsichtsbehörden einen umfassenden Katalog von Untersuchungs- und Abhilfebefugnissen zur Verfügung, um die Einhaltung datenschutzrechtlicher Bestimmungen durchzusetzen. Neben diesen verwaltungsrechtlichen Maßnahmen können Verstöße auch mit hohen Geldbußen sanktioniert werden.

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren (Art. 58 DS-GVO)

Gegenüber Verantwortlichen und Auftragsverarbeitern können vorsorgliche Warnungen ausgesprochen werden, wenn diese Datenverarbeitungen beabsichtigen, die voraussichtlich einen Verstoß gegen die Grundverordnung darstellen, bzw. Verwarnungen, wenn mit Datenverarbeitungen bereits gegen die Grundverordnung verstoßen wurde. Darüber hinaus können Verantwortliche und Auftragsverarbeiter künftig im Rahmen eines förmlichen Verwaltungsaktes von den Aufsichtsbehörden angewiesen werden, Betroffenenrechten zu entsprechen, Datenverarbeitungen mit der Grundverordnung in Einklang zu bringen sowie von einem Datenschutzverstoß betroffene Personen entsprechend zu benachrichtigen. Des Weiteren ist künftig auch die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation möglich. Die Befugnis der Aufsichtsbehörden, Beschränkungen und Verbote von Datenverarbeitungen und die Berichtigung oder Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anzuord-

nen, bleibt unberührt. Nicht zuletzt können mit Inkrafttreten der Grundverordnung Zertifizierungen seitens der Aufsichtsbehörden selbst widerrufen oder Zertifizierungsstellen angewiesen werden, erteilte Zertifizierungen zu widerrufen oder neue Zertifizierungen nicht zu erteilen.

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden.

Zu beachten ist, dass sich die genannten behördlichen Maßnahmen zukünftig nicht nur gegen den Verantwortlichen selbst, sondern auch gegen Auftragsverarbeiter richten können.

Die Aufsichtsbehörden haben umfassende Untersuchungsbefugnisse, wobei den Verantwortlichen und auch Auftragsverarbeiter Mitwirkungspflichten treffen. Insbesondere können die Aufsichtsbehörden den Verantwortlichen und Auftragsverarbeiter sowie deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlich sind.

Alle Anordnungen können mit Zwangsmitteln, wie Zwangsgeldern, durchgesetzt werden. Rechtsschutz bei Zweifeln an der Rechtmäßigkeit der Anordnungen der Aufsichtsbehörde ist wie bisher auch im verwaltungsgerichtlichen Verfahren gewahrt.

Verhängung von Geldbußen (Art. 83 DS-GVO)

Zusätzlich zu oder anstelle all dieser Maßnahmen können Verstöße gegen die Grundverordnung mit Geldbußen geahndet werden.

Der Rahmen für die Geldbußen wird mit der DS-GVO deutlich erhöht. Dies trägt der gestiegenen Bedeutung des Datenschutzes Rechnung. So können Geldbußen von bis zu 10.000.000 EUR bzw. bei Unternehmen bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden (z. B. ist eine weitere erwähnenswerte Neuerung gegenüber der aktuellen Rechtslage, dass unter dem Regime der DS-GVO auch ein Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten mit einer Geldbuße geahndet werden kann). Bei bestimmten, besonders schwerwiegenden Verstößen, darunter Verstöße gegen die Datenverarbeitungsgrundsätze und gegen die Betroffenenrechte oder im Falle einer Verarbeitung ohne Rechtsgrundlage, sind Geldbußen von bis zu 20.000.000 EUR möglich. Gegen Unternehmen kann diese Grenze sogar noch überschritten

werden, nämlich bis zu 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Für den Fall der Nichtbefolgung einer Anweisung der Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO ist ebenfalls die Verhängung einer Geldbuße von bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen. In allen drei Fallgestaltungen richtet sich die maximale Obergrenze für die Geldbuße danach, welcher der Beträge höher ist.

Hierbei geht die DS-GVO von einem gegenüber Art. 4 Nr. 18 DS-GVO erweiterten Unternehmensbegriff aus. Wie der Begriff „Unternehmen“ im Zusammenhang mit dem Bußgeldverfahren zu verstehen ist, ist Erwägungsgrund (ErwGr.) 150 der DS-GVO zu entnehmen. Danach gilt der aus dem Kartellrecht entlehnte weite, funktionale Unternehmensbegriff nach Art. 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Dies hat zur Folge, dass Mutter- und Tochtergesellschaften als wirtschaftliche Einheit betrachtet werden, so dass bei der Bemessung des Bußgeldes der Gesamtumsatz der Unternehmensgruppe zu Grunde gelegt wird.

Nach dem Wortlaut der DS-GVO reicht es für die Zurechnung eines Verstoßes zu einem Unternehmen aus, dass ein Beschäftigter des Unternehmens oder auch ein für das Unternehmen agierender externer Beauftragter gehandelt hat. Die Zurechnung ist damit nicht mehr wie bisher (vgl. § 30 OWiG) auf Handlungen gesetzlicher Vertreter oder anderer Leitungspersonen des Unternehmens begrenzt.

Für die Zumessung der Geldbußen gilt zuvörderst der Grundsatz, dass die Geldbußen wirksam, verhältnismäßig und abschreckend sein müssen. Art. 83 Abs. 2 S. 2 DS-GVO enthält eine Auflistung von Kriterien, die bei der Entscheidung über die Verhängung und die Höhe einer Geldbuße (ggf. auch einem Absehen davon, vgl. ErwGr. 148) gebührend im Einzelfall berücksichtigt werden sollen. Neben Art, Schwere und Dauer des Verstoßes ist unter anderem auch zu berücksichtigen, welche Art von Daten verarbeitet wurde sowie ob früher angeordnete Maßnahmen vom Verantwortlichen eingehalten wurden. Zu berücksichtigen ist künftig auch die Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere, ob und wie die Verantwortlichen mit den Aufsichtsbehörden zusammengearbeitet haben, um Verstößen abzuhelfen und ihre möglichen nachteiligen Auswirkungen zu mindern, und ob sie die Verstöße eigenständig mitgeteilt haben. Ferner ist auch der Grad der Verantwortung des Verantwortlichen bzw. Auftragsverarbeiters unter Berücksichtigung der von ihm getroffenen technischen und organisatorischen Maßnahmen ein zu berücksichtigendes Kriterium. Mithin wird im Einzelfall zu überprüfen sein, inwieweit ein Unternehmen im Rahmen seiner internen Orga-

nisation, etwa durch Ausgestaltung seiner Strukturen, Arbeitsprozesse und Kontrollmechanismen, Vorkehrungen getroffen hat, die dazu dienen, die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen, bzw. inwieweit die interne Organisation diesbezüglich Mängel aufweist. Zudem können jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste, Berücksichtigung finden.

Abzuwarten bleibt, in welcher Form der Europäische Datenschutzausschuss seinen Auftrag aus Art. 70 Abs. 1 lit. k DS-GVO umsetzen wird. Danach obliegt ihm die Aufgabe, Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen gemäß Art. 83 DS-GVO zu erlassen.

19.3
Kurzpapier Nr. 3

Verarbeitung personenbezogener Daten für Werbung

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.

Keine Detailregelung für Werbung

Mit der DS-GVO fallen alle detaillierten Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Verarbeitung personenbezogener Daten für werbliche Zwecke weg.

Werbung nach Interessenabwägung

Grundlage für die Beurteilung der Zulässigkeit von Werbung ist in Zukunft, abgesehen von einer Einwilligung, eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Ausgangspunkt für die zu treffende Abwägungsentscheidung ist 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."

Ferner gibt ErwGr. 47 DS-GVO im Rahmen der durchzuführenden Interessenabwägung vor, die „vernünftigen Erwartungen der betroffenen Person", die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in den Abwägungsprozess einzubeziehen.

Wann diese Voraussetzungen vorliegen, ist derzeit noch nicht abschließend geklärt. Dem Working Paper der Art. 29-Datenschutzgruppe (WP 217, S. 51), das sich allerdings auf die Datenschutzrichtlinie 95/46/EG bezieht, können insoweit erste Interpretationshinweise entnommen werden.

Die vernünftigen Erwartungen der betroffenen Person werden bei Maßnahmen zur werblichen Ansprache maßgebend durch die Informationen nach Art. 13, 14 DS-GVO zu den Zwecken der Datenverarbeitung bestimmt werden.

Informiert der Verantwortliche transparent und umfassend über eine vorgesehene werbliche Nutzung der Daten, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden.

Insoweit ist im Rahmen der Interessenabwägung zu berücksichtigen, dass die von Werbung betroffenen Personen ein jederzeitiges und umfassendes Widerspruchsrecht haben (Art. 21 Abs. 2 DS-GVO), auf das sie ausdrücklich hinzuweisen sind (Art. 21 Abs. 4 DS-GVO). Der Werbewiderspruch hat nach Art. 21 Abs. 3 DS-GVO zur Folge, dass personenbezogene Daten für Werbezwecke nicht mehr verarbeitet, insbesondere verwendet werden dürfen. Im Übrigen ist zu berücksichtigen, ob die betroffene Person bereits Kunde des Verantwortlichen ist oder dessen Dienste nutzt (ErwGr. 47 DS-GVO). Ferner sind bei der Interessenabwägung auch die 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)

Diese Grundsätze sprechen jedenfalls dagegen, Profile zur werblichen Ansprache (Werbescores) zu erstellen, die z. B. Informationen aus sozialen Netzwerken berücksichtigen.

Eingriffsintensivere Maßnahmen wie Profilbildung sprechen eher dafür, dass ein Interesse der betroffenen Person am Ausschluss der Datenverarbeitung überwiegt.

Unabhängig von der Interessenabwägung müssen die Informationspflichten nach den Art. 13, 14 DS-GVO eingehalten werden.

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.).

Besondere Grenzen aus § 7 UWG

Auch nach neuem Recht wird die Interessenabwägung bei der Nutzung der Kontaktdaten von Verbrauchern für Telefon- und Faxwerbung dazu führen, dass diese weiterhin nur mit einer vorherigen ausdrücklichen Einwilligung erlaubt ist. Alles andere wäre im Hinblick auf die klaren Regelungen in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG) mit den vernünftigen Erwartungen der Betroffenen (ErwGr. 47 DS-GVO) nicht zu vereinbaren.

Ebenso ist eine Kontaktdatennutzung für E-Mail- und SMS-Werbung außerhalb einer Einwilligung nur im Fall der Eigenwerbung bei Bestandskunden unter den Maßgaben von § 7 Abs. 3 UWG zulässig.

Im Übrigen bleibt abzuwarten, inwieweit die geplante neue ePrivacy-Verordnung im Bereich der elektronischen Werbung konkrete Regelungen (z. B. ausschließliche Opt-in-Lösung) für werbliche Ansprachen enthalten wird.

Fortgeltung von Einwilligungen

Bisher erteilte Einwilligungen wirken nach ErwGr. 171 der DS-GVO fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen. Die im Wirtschaftsleben EU-weit vorhandenen Einwilligungen sind auf ihre Wirksamkeit hin zu überprüfen. Dabei ist u.a. von Bedeutung, ob auf Grundlage der neuen Anforderungen nach Art. 7 Abs. 4 der DS-GVO eine freiwillige Erklärung abgegeben und dass die Altersgrenze für die Einwilligungsfähigkeit bei Inanspruchnahme von Diensten der Informationsgesellschaft nach Art. 8 Abs. 1 der DS-GVO berücksichtigt wurde.

„Koppelungsverbot“ bei Einwilligungen für Werbung

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).

Bei „kostenlosen“ Dienstleistungsangeboten, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen“ (z. B. kostenloser E-Mail-Account gegen Zustimmung für Newsletter-Zusendung als „Gegenfinanzierung“), muss diese vertraglich ausbedungene Gegenleistung des Nutzers bei Vertragsabschluss klar und verständlich dargestellt werden. Nur dann besteht keine Notwendigkeit mehr für eine Einwilligung.

Ausblick für den künftigen Umgang mit personenbezogenen Daten für Werbung

Soweit Werbung nicht auf einer wirksamen Einwilligung der betroffenen Person beruht, wird für die Zulässigkeit von Werbung in Zukunft fast ausschließlich die nach Art. 6 Abs. 1 lit. f DS-GVO vorgeschriebene Interessenabwägung maßgeblich sein.

Inwieweit es in Europa gelingen wird, die in Deutschland entwickelten Maßstäbe auch unter Geltung der DS-GVO aufrechtzuerhalten, wird sich zeigen. Anzustreben sind für diesen Bereich möglichst EU-weite Verhaltensregeln. Sollte das nicht für die wesentlichen Bereiche der

Werbung gelingen, wird mit Leitlinien des Europäischen Datenschutzausschusses auch zu diesem Thema zu rechnen sein.

19.4
Kurzpapier Nr. 4

Datenübermittlung in Drittländer

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 DS-GVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen vor: Art. 44 - 49. Länder außerhalb der EU/des EWR werden in der DS-GVO als „Drittländer“ bezeichnet, in der Praxis wird auch der Begriff „Drittstaat“ verwendet. Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den in den Art. 45 ff. geregelten spezifischen Anforderungen an Datenübermittlungen in Drittländer auch alle übrigen Anforderungen der DS-GVO (z. B. Art. 9 Abs. 3) an die in Rede stehende Datenverarbeitung eingehalten werden (1. Stufe). Steht nach diesem Prüfungsschritt einer Verarbeitung nichts entgegen, müssen gemäß Art. 44 zusätzlich die spezifischen Anforderungen der Art. 45 ff. an die Übermittlung in Drittländer beachtet werden (2. Stufe; „2-Stufen-Prüfung“). Dies gilt auch bei einer Weiterübermittlung der personenbezogenen Daten durch die empfangende Stelle im Drittland (Art. 44 S. 1 2. HS (siehe auch Erwägungsgrund (ErwGr.) 101)).

Die DS-GVO sieht für Datentransfers in Drittländer folgende Möglichkeiten vor (für öffentliche Stellen gelten im Einzelfall ergänzende Regelungen):

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO)**
- **Vorliegen geeigneter Garantien (Art. 46 DS-GVO) oder**
- **Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO).**

1. Feststellung der Angemessenheit des Datenschutzniveaus im Drittstaat durch die Kommission (Art. 45 DS-GVO)

Die Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist. Eine Datenübermittlung auf Grundlage eines solchen Angemessenheitsbeschlusses bedarf keiner weiteren Genehmigung durch die für den Verantwortlichen oder Auftragsverarbeiter zuständige nationale Aufsichtsbehörde.

Die DS-GVO sieht eine Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse vor (Art. 46 Abs. 5 S. 2).

Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt [C(2016) 4176 final)].

2. Vorliegen geeigneter Garantien (Art. 46 DS-GVO)

Eine Datenübermittlung in ein Drittland ist weiter zulässig, wenn der Verantwortliche oder Auftragsverarbeiter geeignete Garantien zur Gewährleistung eines angemessenen Schutzniveaus vorgesehen hat. Folgende Garantien kommen in Betracht:

a) Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) (Art. 46 Abs. 2 lit. b, Art. 47)

Verbindliche interne Datenschutzvorschriften (BCR) wurden schon bisher in der Praxis verwendet und sind nun in der DS-GVO (anders als in der noch geltenden EU-Datenschutzrichtlinie 95/46/EG) ausdrücklich als Möglichkeit zur Erbringung „geeigneter Garantien“ für Datenübermittlungen in Drittländer geregelt. Sie können vor allem bei international tätigen Konzernen mit internem Datenfluss (auch) in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest. Die BCR müssen einen Schutz bieten, der im Wesentlichen der DS-GVO

entspricht. Der Mindestinhalt ist in Art. 47 Abs. 2 festgelegt. Zudem müssen die BCR für alle betreffenden Mitglieder der Unternehmensgruppe rechtlich bindend sein und den betroffenen Personen durchsetzbare Rechte gewähren (Art. 47 Abs. 1 lit. a und b). Die Genehmigung der BCR erfolgt gemäß dem Kohärenzverfahren durch die zuständige Aufsichtsbehörde (Art. 47 Abs. 1). Die konkreten Datenübermittlungen auf Grundlage der BCR werden dann nicht mehr einzeln genehmigt.

b) Standarddatenschutzklauseln der Kommission oder einer Aufsichtsbehörde (Art. 46 Abs. 2 lit. c und d)

Schließen der Datenexporteur und der Datenimporteur einen Vertrag unter Verwendung der Standarddatenschutzklauseln der Kommission, ist der darauf basierende Datentransfer ohne weitere Genehmigung durch die Aufsichtsbehörde zulässig (vorbehaltlich der weiteren Anforderungen nach der DS-GVO). Auch den Aufsichtsbehörden ist es möglich, eigene Standarddatenschutzklauseln zu entwerfen. Diese bedürfen der Abstimmung im Kohärenz-verfahren und sind anschließend von der Kommission förmlich zu genehmigen.

Die bereits bestehenden EU-Standardvertragsklauseln gelten gemäß Art. 46 Abs. 5 S. 2 ausdrücklich fort. Sofern die Standarddatenschutzklauseln in unveränderter Form verwendet werden, sind die Datenübermittlungen genehmigungsfrei. Dies gilt auch noch dann, wenn ihnen weitere Klauseln oder zusätzliche Garantien hinzugefügt werden, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den Standarddatenschutzklauseln stehen und die Grundrechte und Grundfreiheiten der betroffenen Personen nicht beschneiden (ErwGr. 109). Bei solchen Hinzufügungen sollten Unternehmen jedoch eine gewisse Vorsicht walten lassen, da im Falle eines inhaltlichen Widerspruchs zu den Standarddatenschutzklauseln die Übermittlung nicht mehr genehmigungsfrei ist.

c) Genehmigte Verhaltensregeln und genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. e und f)

Neu hinzugekommen ist die Möglichkeit, Datenübermittlungen auf Grundlage von branchenspezifischen Verhaltensregeln gemäß Art. 40 zu legitimieren, sofern diese mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters versehen sind und von der zuständigen Aufsichtsbehörde genehmigt worden sind.

Auch Zertifizierungen nach Art. 42 können nun zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters als rechtliche

Grundlage für einen Datentransfer in ein Drittland herangezogen werden, wenn die Zertifizierungsmechanismen zuvor genehmigt worden sind.

Die europäischen Aufsichtsbehörden werden in der Folgezeit die für eine praktische Anwendung dieser Instrumente notwendigen weiteren Einzelheiten im Hinblick auf rechtliche Rahmenbedingungen und Verfahrensfragen erarbeiten.

d) Einzeln ausgehandelte Vertragsklauseln (Art. 46 Abs. 3)

Ebenso können einzeln ausgehandelte individuelle Vertragsklauseln eine Datenübermittlung in ein Drittland legitimieren, allerdings nur nach Genehmigung der Aufsichtsbehörde und Durchführung des Kohärenzverfahrens nach Art. 63.

e) Rechte der betroffenen Personen

Gemäß Art. 46 Abs. 1 a. E. ist es bei allen in Betracht kommenden geeigneten Garantien im Sinne von Art. 46 zusätzlich erforderlich, den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe einzuräumen.

3. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)

Eine Datenübermittlung kann in einer Reihe besonderer, vom Gesetz explizit genannter und abschließender Fälle, auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Kommission noch geeignete Garantien vorliegen. Die hierfür von der DS-GVO definierten Ausnahmetatbestände sind gemäß ihrem Ausnahmecharakter eng auszulegen.

a) Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a)

Eine wirksame Einwilligung der betroffenen Person in die Datenübermittlung in ein Drittland setzt zunächst eine ausdrückliche Einwilligung in die Weitergabe ihrer Daten für den konkreten Fall voraus. Weiter ist die betroffene Person vorher explizit über bestehende mögliche Risiken derartiger Datenübermittlungen aufzuklären, d. h. insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte ggf. nicht durchgesetzt werden können. Auch ist die betroffene Person darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann (Art. 7 Abs. 3).

b) Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b und c)

Eine Datenübermittlung in ein Drittland ist (vorbehaltlich der weiteren Anforderungen der DS-GVO) zulässig, wenn und soweit die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person oder zum Abschluss oder zur Erfüllung eines Vertrages im Interesse der betroffenen Person erforderlich ist. Wesentlich ist hier jeweils die strikte Erforderlichkeit gerade dieser Datenübermittlung zur Erfüllung des Vertragszwecks.

c) Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d)

Die Übermittlung kann auch zulässig sein, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. In Betracht kommen nur wichtige öffentliche Interessen, die im Recht der Europäischen Union oder des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sind (Art. 49 Abs. 4). Wie aus Erwägungsgrund 112 hervorgeht, hatte der Gesetzgeber insoweit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit im Auge, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden.

d) Verfolgung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e)

Auch die Verfolgung von Rechtsansprüchen kann eine Datenübermittlung legitimieren, wenn die Datenübermittlung hierzu erforderlich ist. In Erweiterung der bisherigen Regelung im BDSG kommt auch die Geltendmachung von Rechtsansprüchen in außergerichtlichen Verfahren in Betracht (ErwGr. 111).

e) Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 lit. f)

Ist die betroffene Person aus physischen oder rechtlichen Gründen nicht in der Lage, ihre Einwilligung zu erteilen, darf die Datenübermittlung dennoch durchgeführt werden, soweit dies zum Schutz ihrer lebenswichtigen Interessen oder derjenigen anderer Personen erforderlich ist.

f) Wahrung zwingender berechtigter Interessen (Art. 49 Abs. 1 UAbs. 2 S. 1)

Im Einzelfall kann eine Datenübermittlung in ein Drittland legitimiert sein, wenn ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung besteht, die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Anzahl von Personen betrifft und keine überwie-

genden schutzwürdigen Interessen oder Rechte und Freiheiten der betroffenen Person entgegenstehen und der Verantwortliche durch geeignete Garantien den Schutz personenbezogener Daten gewährleistet. Voraussetzung für diese Übermittlungserlaubnis ist ein zwingendes berechtigtes Interesse des Verantwortlichen an der Übermittlung, dem eine herausgehobene und besondere Bedeutung zukommt. Zudem muss die Übermittlung unbedingt erforderlich sein zur Verfolgung dieses berechtigten Interesses. Die Übermittlung darf sich nicht bereits auf einen der oben genannten Erlaubnistatbestände stützen lassen. Wird eine Übermittlung in ein Drittland auf Grundlage eines zwingenden berechtigten Interesses in einem absoluten Einzelfall durchgeführt, ist sowohl die Aufsichtsbehörde als auch die betroffene Person hierüber zu informieren (Art. 49 Abs. 1 UAbs. 2 S. 2 und 3).

19.5
Kurzpapier Nr. 5

Datenschutz-Folgenabschätzung nach Art. 35 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.

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten entstehen Risiken für die betroffenen Personen. Deswegen sieht die DS-GVO unabhängig von sonstigen Voraussetzungen für die Verarbeitung vor, dass durch geeignete Abhilfemaßnahmen [insbesondere durch technische und organisatorische Maßnahmen (TOMs)] diese Risiken eingedämmt werden. Das Instrument einer Datenschutz-Folgenabschätzung (DSFA) kann hierfür systematisch eingesetzt werden.

Was ist eine Datenschutz-Folgenabschätzung nach DS-GVO?

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr. 84, 90). Zum Begriff des Risikos, der ein zentrales Konzept der DS-GVO ist, wird es ein eigenes Kurzpapier geben.

Verarbeitungsvorgang als Ankerpunkt

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.

Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr. 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

Erforderlichkeit einer DSFA

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“). Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht zwingend erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren.

Art. 35 Abs. 3 DS-GVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO führen. Aufbauend auf den Leitlinien der Artikel 29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste mit

Verarbeitungstätigkeiten, bei denen eine DSFA durchzuführen ist, veröffentlichen. Auch zur Durchführung der Schwellwertanalyse werden künftig Hinweise zur Verfügung gestellt.

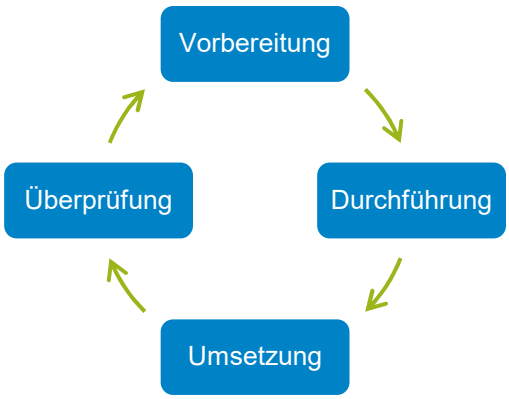
Zeitpunkt der Durchführung einer DSFA

Eine DSFA ist vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen. Da eine DSFA meist nicht ad hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig, beispielsweise unterstützt durch ein allgemeines Datenschutz-Managementsystem, auf den Weg gebracht werden.

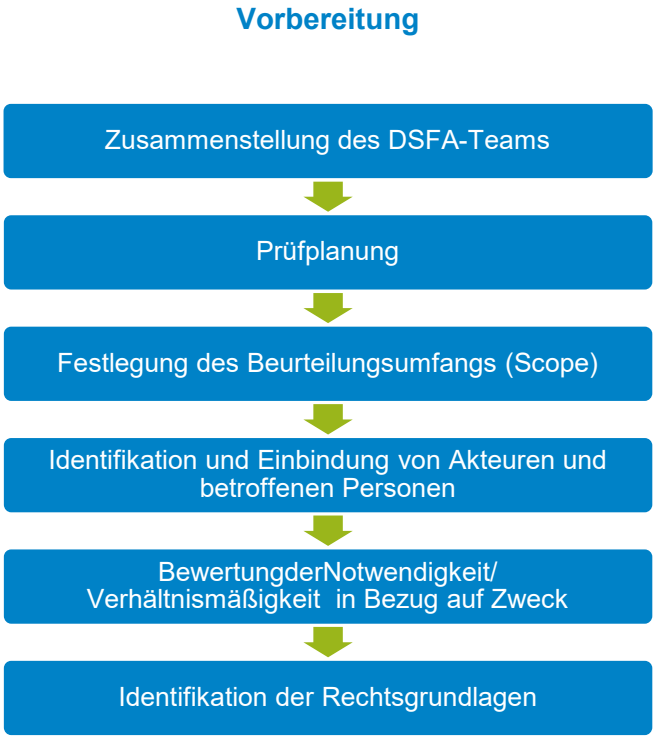
Wie kann eine DSFA durchgeführt werden?

Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DS-GVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Bei der verwendeten Methode wird dem Verantwortlichen mehr Spielraum gelassen. Werden bestehende Methoden oder Standards eingesetzt, ist zu beachten, dass die Anforderungen der DS-GVO immer vorrangig zu behandeln sind.

Eine DSFA ist kein einmaliger Vorgang. Sollten sich z. B. neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA bisher nicht berücksichtigt wurden, so ist die DSFA zu überprüfen und ebenso anzupassen. Um dies zu garantieren, wird ein stetiger, iterativer Prozess der Überprüfung und Anpassung empfohlen:



Die Bestandteile der Hauptprozessschritte werden im Einzelnen nachfolgend dargestellt.



1. Zusammenstellung des DSFA-Teams

Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Risikoermittlung und Fachprozesse mitbringt. Der Datenschutzbeauftragte steht diesem während des gesamten Prozesses beratend zur Seite. Es kann sinnvoll oder notwendig sein, z. B. Auftragsverarbeiter oder Hersteller von IT-Systemen ebenfalls mit einzubeziehen.

2. Prüfplanung

Da eine DSFA meist ein komplexer Prozess ist, der viele Mitwirkende einbindet, ist eine Prüfplanung (z. B. mit Methoden des Projektmanagements) empfehlenswert.

3. Festlegung des Beurteilungsumfangs (Scope)

Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-)Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen zu beschreiben. Wesentlich ist es, die beabsichtigten Zwecke der Verarbeitungsvorgänge festzuhalten.

4. Identifikation und Einbindung von Akteuren und betroffenen Personen

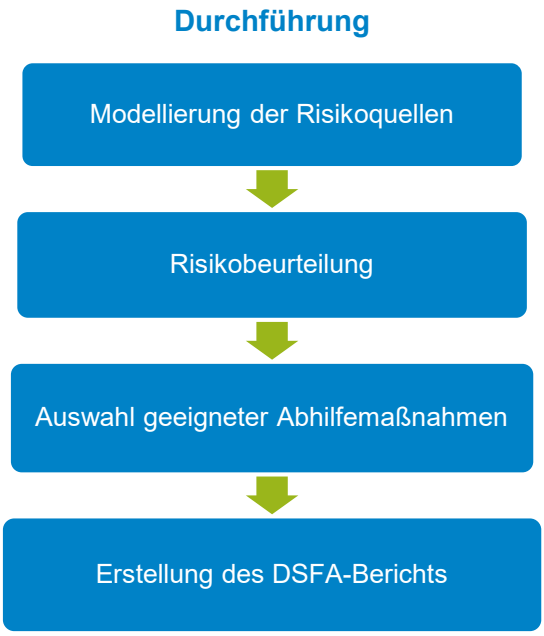
Die Akteure und betroffenen Personen sind zu identifizieren. Bei der Durchführung der DSFA zieht der Verantwortliche den Datenschutzbeauftragten zurate (Art. 35 Abs. 2 DS-GVO). Ggf. holt der Verantwortliche den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung ein (Art. 35 Abs. 9 DS-GVO). Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung, z. B. von Betriebsräten.

5. Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf ihren Zweck

Die im vorigen Schritt beschriebenen Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu dem angestrebten Zweck steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der Betroffenen weniger stark eingreifen. Ggf. nimmt der Verantwortliche eine Anpassung der Verarbeitungsvorgänge vor, z. B. durch Beschränkung der zu verarbeitenden Daten oder durch Änderung der beteiligten Akteure oder eingesetzten Technologien.

6. Identifikation der Rechtsgrundlagen

Aufbauend auf dem vorigen Schritt können sodann die Rechtsgrundlagen für die zu bewertenden Verarbeitungsvorgänge bestimmt und dokumentiert werden.



7. Modellierung der Risikoquellen

Die Quellen des Risikos für die Rechte und Freiheiten natürlicher Personen müssen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen, und welches ihre Beweggründe und möglichen Ziele sein können. Anhand dessen können die damit zusammenhängenden Eintrittswahrscheinlichkeiten ermittelt werden.

8. Risikobeurteilung

Aufbauend auf den vorherigen Schritten wird bestimmt, ob in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Ihre Schwere sowie die jeweilige Eintrittswahrscheinlichkeit sind dabei zu berücksichtigen (ErwGr. 75 f.).

9. Auswahl geeigneter Abhilfemaßnahmen

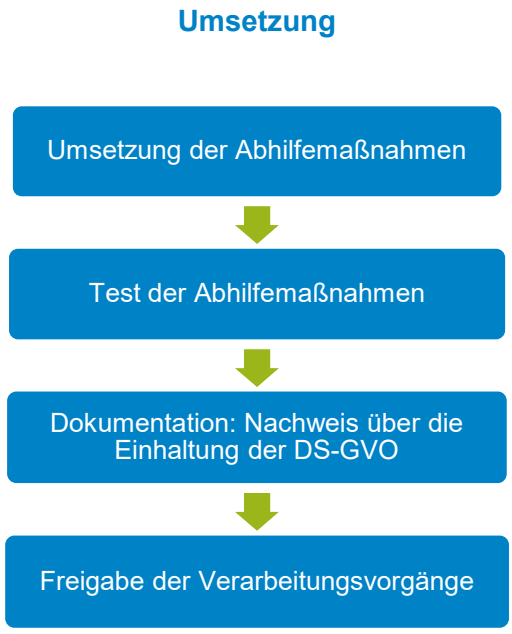
Die ermittelten Risiken müssen durch geeignete Abhilfemaßnahmen (insbesondere durch TOMs) eingedämmt werden. Eine Auswahl sowie Planung der Umsetzung der Maßnahmen findet statt. Dabei wird den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen. Verbleibende Restrisiken werden ermittelt und dokumentiert.

10. Erstellung des DSFA-Berichts

Der DSFA-Bericht enthält gem. Art. 35 Abs. 7 DS-GVO jedenfalls die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Der Bericht ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Er kann sich dabei an den hier dargestellten Phasen orientieren. Der DSFA-Bericht dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Weitere Schritte nach Durchführung der DSFA

Die folgenden Schritte dienen der Implementierung der Abhilfemaßnahmen und sollten nicht lediglich linear durchlaufen werden, sondern eine Rückkoppelung der jeweiligen Ergebnisse im Sinne eines iterativen Vorgehens ermöglichen. Beispielsweise können durch eine Maßnahme weitere Verarbeitungsvorgänge nötig werden, für die wiederum etwaige Risiken zu betrachten sind.



11. Umsetzung der Abhilfemaßnahmen

Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Risikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DS-GVO genügen.

12. Test der Abhilfemaßnahmen

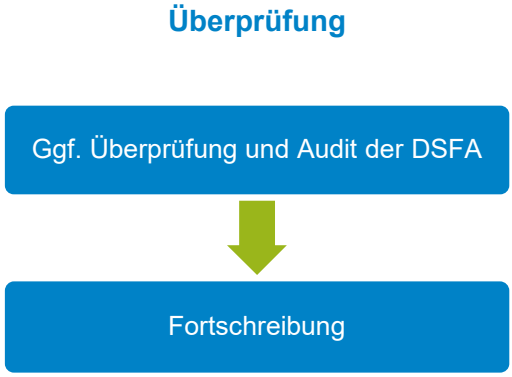
Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

13. Dokumentation: Nachweis über die Einhaltung der DS-GVO

Gem. Art. 5 Abs. 2 DS-GVO hat der Verantwortliche eine umfassende Dokumentations- und Rechenschaftspflicht, durch die die Einhaltung der DS-GVO insgesamt nachgewiesen werden soll. Der DSFA-Bericht und eine Bestätigung der Wirksamkeit der umgesetzten Maßnahmen dienen als Bausteine zur Erfüllung dieser Pflicht.

14. Freigabe der Verarbeitungsvorgänge

Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Verantwortlichen freigegeben werden.



15. Ggf. Überprüfung und Audit der DSFA

Um eine ordnungsgemäße Durchführung sicherzustellen, kann es sinnvoll sein, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Auch könnte der Datenschutzbeauftragte, der gemäß Art. 35 Abs. 2 DS-GVO sowieso einzubeziehen ist, die DSFA abschließend prüfen und das Ergebnis der Leitungsebene des Verantwortlichen mitteilen.

16. Fortschreibung

Die DSFA ist kein strikt linearer oder abgeschlossener Prozess. Vielmehr muss die Einhaltung der DS-GVO während der gesamten Dauer der Verarbeitungsvorgänge fortlaufend überwacht werden. Hierfür bietet sich ein Datenschutz-Managementsystem an. Spätestens wenn sich das mit der Verarbeitung verbundene Risiko ändert, muss erneut eine DSFA durchgeführt werden.

Umgang mit hohen Restrisiken

Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 DS-GVO der Verantwortliche die zuständige Aufsichtsbehörde konsultieren. Er trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DS-GVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

Fazit

Die Datenschutz-Folgenabschätzung ist ein sinnvolles Instrument zur systematischen Risikoeindämmung und stellt eine der wichtigsten Neuerungen der DS-GVO gegenüber dem BDSG dar. Rechtzeitig auf den Weg gebracht hilft sie nicht nur, die eigenen Prozesse bei der Verarbeitung personenbezogener Daten besser zu verstehen, sondern auch die Pflichten nach der Grundverordnung umzusetzen.

19.6
Kurzpapier Nr. 6

Auskunftsrecht der betroffenen Person, Art. 15 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.

Auskunftsrecht als zentrales Recht zur Schaffung von Transparenz

Wie schon nach der bisherigen Rechtslage haben betroffene Personen das Recht mit formlosem Antrag und ohne Begründung von einem Verantwortlichen Auskunft über dort gespeicherte personenbezogene Daten zu verlangen. Die Auskünfte können es beispielsweise erleichtern, gezielt weitere Rechte, wie auf Berichtigung, Löschung oder Einschränkung der Verarbeitung („Sperrung“), geltend zu machen.

Umfang des Auskunftsrechts

Nach Art. 15 Abs. 1 DS-GVO steht der betroffenen Person ein abgestuftes Auskunftsrecht zu.

Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche entweder keine Daten zu dieser Person verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert hat.

Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

Weiterhin sind bei der Datenauskunft vom Verantwortlichen nach Art. 15 Abs. 1 DS-GVO vor allem noch folgende Informationen mitzuteilen:

– Verarbeitungszwecke,
– Kategorien personenbezogener Daten, die verarbeitet werden (mit Gruppenbezeichnungen wie Gesundheitsdaten, Bonitätsdaten usw.),
– Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden,
– geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer,
– Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
– Widerspruchsrecht gegen diese Verarbeitung nach Art. 21 DS-GVO,
– Beschwerderecht für die betroffene Person bei der Aufsichtsbehörde,
– Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden, und

– das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren.

Im Falle der Datenübermittlung in Drittländer ist über die insoweit gegebenen Garantien gemäß Art. 46 DS-GVO zu informieren (z. B. vereinbarte Standard-Datenschutzklauseln, verbindliche interne Datenschutzvorschriften, d. h. BCR). Keine Drittländer sind die EU-Mitgliedsstaaten und die Vertragsstaaten des EWR.

Form der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person kann nach Art. 12 Abs. 1 Sätze 2 und 3 DS-GVO je nach Sachverhalt schriftlich, elektronisch oder – auf Wunsch der betroffenen Person – mündlich erfolgen. Der Verantwortliche stellt eine Kopie der Daten zur Verfügung (Art. 15 Abs. 3 Satz 1 DS-GVO). Stellt die betroffene Person ihren Auskunftsantrag elektronisch, ist die Auskunft nach Art. 15 Abs. 3 Satz 2 DS-GVO in einem gängigen elektronischen Format zur Verfügung zu stellen (z. B. im PDF-Format). Als datenschutzfreundlichste Gestaltung wird in Erwägungsgrund (ErwGr.) 63 Satz 4 ein vom Verantwortlichen eingerichteter Fernzugriff der betroffenen Person auf ihre eigenen Daten bezeichnet. Alle Kommunikationswege müssen angemessene Sicherheitsanforderungen erfüllen.

Frist für die Auskunftserteilung

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 DS-GVO unverzüglich erfolgen, spätestens aber innerhalb eines Monats; nur in begründeten Ausnahmefällen kann die Monatsfrist überschritten werden, worüber die betroffene Person zu informieren ist (Art. 12 Abs. 3 Satz 3 DS-GVO). Der Verantwortliche muss (vorbereitend) geeignete organisatorische Maßnahmen treffen, damit die betroffene Person eine beantragte Auskunft zeitnah und in verständlicher Form erhalten kann (Art. 12 Abs. 1 Satz 1 und Art. 5 Abs. 2 DS-GVO).

Kosten der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person (z. B. als Kopie) muss durch den Verantwortlichen regelmäßig unentgeltlich erfolgen, Art. 12 Abs. 5 Satz 1 DS-GVO. Für weitere Kopien kann er ein angemessenes Entgelt fordern. Außerdem kann bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt für die Auskunft verlangt werden (Art. 12 Abs. 5 Satz 2, ErwGr. 63).

Identitätsprüfung

Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag).

Grenzen des Auskunftsrechts

Bei einer großen Menge von gespeicherten Informationen über die betroffene Person kann der Verantwortliche verlangen, dass präzisiert wird, auf welche Informationen oder Verarbeitungsvorgänge sich das Auskunftsersuchen konkret bezieht (ErwGr. 63 Satz 7). Das kann z. B. bei Banken oder Versicherungen mit umfangreichen Vertragsbeziehungen zu der betroffenen Person der Fall sein.

Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht führen (Art. 12 Abs. 5 S. 2 DS-GVO). Die betroffene Person muss jedoch (und zwar kostenfrei) ihr Recht in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können (ErwGr. 63). Eine Ablehnung oder Kostenerstattung kommt daher nur in Ausnahmefällen in Betracht. Der Verantwortliche trägt die Beweislast für das Vorliegen eines unbegründeten oder exzessiven Antrags (Art. 12 Abs. 5 Satz 3 DS-GVO). Er muss der betroffenen Person in der Regel die Gründe für die Verweigerung der Auskunft mitteilen und sie über Rechtsschutzmöglichkeiten informieren (Art. 12 Abs. 4 DS-GVO).

Das BDSG-neu enthält in § 34 noch weitere Eingrenzungen des Auskunftsrechts, insbesondere für Archivdaten und Protokollierungsdaten.

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 eine Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Beachtung Rechte Dritter

Die Auskunftserteilung an die betroffene Person darf nach Art. 15 Abs. 4 DS-GVO sowie ErwGr. 63 Satz 5 die Rechte des Verantwortlichen oder anderer Personen nicht beeinträchtigen, was bei Geschäftsgeheimnissen oder bei Daten mit Bezug auch auf andere Personen der Fall sein kann. Dies darf im Ergebnis aber nicht dazu führen, dass jegliche Auskunft verweigert wird.

Rechtfolgen bei Verstoß

Unterlassene oder nicht vollständige Auskunftserteilungen an betroffene Personen sind nach Art. 83 Abs. 5 lit. b DS-GVO mit einer hohen Geldbuße bedroht.

Empfehlung

Es ist für Verantwortliche ratsam, rechtzeitig im eigenen Interesse organisatorische Vorkehrungen für zügige und korrekte Auskunftserteilungen zu treffen.

19.7
Kurzpapier Nr. 7

Marktortprinzip: Regelungen für außereuropäische Unternehmen

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.

Regelung des Marktortprinzips in Art. 3 Abs. 2 DS-GVO

Das Marktortprinzip schließt unter bestimmten Bedingungen auch Unternehmen, die nicht in der EU niedergelassen sind, in den Anwendungsbereich der DS-GVO ein.

Seit In-Kraft-Treten der EU-Datenschutzrichtlinie im Jahr 1995 haben sich neue Fragestellungen zum Anwendungsbereich des europäischen Datenschutzrechts entwickelt, beispielsweise mit Blick auf die fortschreitende Verlagerung von Geschäftsaktivitäten ins Internet (eCommerce). Sie erfordern keine physischen Betriebs- und Organisationsstrukturen in Europa, die als direkter Anknüpfungspunkt für die Anwendbarkeit europäischen Datenschutzrechts dienen könnten.

Der europäische Gesetzgeber erstreckt den Anwendungsbereich des europäischen Datenschutzrechts mit Einführung des Marktortprinzips auf datenschutzrechtlich relevante Geschäftsaktivitäten von Unternehmen, die keine Niederlassungen in der EU besitzen und damit an sich außerhalb des territorialen Anwendungsbereichs nach Art. 3 Abs. 1 DS-GVO liegen würden. Unter den von Art. 3 Abs. 2 lit. a und lit. b DS-GVO festgelegten Bedingungen erstreckt sich der Anwendungsbereich der DSGVO auf Verarbeitungen personenbezogener Daten von Betroffenen, die sich in der EU befinden, ohne Rücksicht auf physische Organisations- oder Betriebsstrukturen von Unternehmen in der EU.

1. Anknüpfungspunkt: Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 lit. a DS-GVO)

Die DS-GVO findet Anwendung, wenn eine Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten. Das Unternehmen muss dies offensichtlich beabsichtigen (vgl. ErwGr. 23). Die Zahlung eines Entgeltes für das Waren- oder Dienstleistungsangebot ist hierbei für die Anwendbarkeit der DS-GVO irrelevant, sondern es sollen explizit auch unentgeltliche Angebote, z. B. Dienstleistungen durch soziale Netzwerke, darunterfallen.

Ein maßgeblicher Anknüpfungspunkt ist die Ausrichtung bestimmter Werbe- bzw. Verkaufsmaßnahmen auf Personen, die sich in der EU befinden. Wann dies der Fall ist, muss anhand von Hilfsfaktoren und Indizien bestimmt werden. Keine ausreichenden Anhaltspunkte hierfür sind etwa allein

– die bloße Abrufbarkeit einer kommerziellen Internetpräsenz, einer E-Mail-Adresse oder sonstiger Kontaktdaten oder
– die Verwendung einer (EU-)Sprache, die in dem Drittstaat, in dem das jeweilige Unternehmen niedergelassen ist, allgemein gebräuchlich ist.

Haftungsausschlüsse (so genannte Disclaimer), die beispielsweise die Anwendbarkeit der DS-GVO beschränken oder ausschließen, lassen wiederum nicht zwingend auf die Nichtanwendbarkeit der DS-GVO schließen.

Andere Faktoren wie

– die Verwendung der Sprache oder Währung eines Mitgliedstaates in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen oder
– die Erwähnung von Kunden oder Nutzern, die sich in der EU befinden,

können darauf hindeuten, dass ein Unternehmen beabsichtigt, den betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten (vgl. ErwGr. 23). Ein Angebot kann auch dann (potentielle) Kunden und Nutzer in der EU adressieren, wenn das jeweilige Waren- oder Dienstleistungsangebot einen hinreichend konkreten personalen Bezug zum Marktgeschehen aufweist. Zur Bestimmung dessen können beispielsweise „Flaggen-Icons“, landesspezifische „Top Level Domains“ oder geographische Referenzen zu den mitgliedstaatlichen Märkten herangezogen werden.

2. Anknüpfungspunkt: Überwachung des Verhaltens von Personen (Art. 3 Abs. 2 lit. b DS-GVO)

Die DS-GVO ist auch dann anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten von betroffenen Personen zu beobachten, soweit dieses Verhalten in der EU erfolgt. Dies ist zum Beispiel dann der Fall, wenn die Internetaktivitäten der betroffenen Person nachvollzogen werden. Eine solche Nachvollziehbarkeit kann auch im Fall der nachfolgenden Erstellung von (Persönlichkeits-)Profilen angenommen werden, wenn

– diese die Grundlage für eine die jeweilige Person betreffende Entscheidung bilden oder
– anhand derer die Vorlieben, Verhaltensweisen oder Gepflogenheiten einer natürlichen Person analysiert oder vorausgesagt werden sollen (vgl. ErwGr. 24).

Dies kann zum Beispiel durch den Einsatz von „Tracking-Cookies“ oder „Browser Fingerprints“ stattfinden. Diese Techniken können auch als Grundlage für die weitere Erstellung persönlicher Profile, etwa zum Zwecke individualisierter bzw. zielgruppenspezifischer Werbung (sog. Behavioural Targeting) dienen.

Weitere Folgen

Außereuropäische Unternehmen, auf deren Verarbeitungstätigkeiten die DS-GVO anwendbar ist, müssen grundsätzlich einen in einem betroffenen Mitgliedstaat niedergelassenen Vertreter benennen. Der Vertreter ist ausdrücklich zu bestellen und schriftlich zu beauftragen, in Bezug auf die sich aus der DS-GVO ergebenden Pflichten an Stelle des Verantwortlichen oder des Auftragsverarbeiters zu handeln. Als Anlaufstelle soll dieser Vertreter einerseits den betroffenen Personen ermöglichen, ihre Betroffenenrechte wirksam geltend zu machen und andererseits die Aufsichtsbehörden in die Lage versetzen, ihre Aufsichtsmaßnahmen effektiv durchzusetzen (Art. 27 DS-GVO, siehe auch ErwGr. 80). Die Pflicht entfällt, wenn die Verarbeitung

– lediglich gelegentlich erfolgt,
– nicht die umfangreiche Verarbeitung sensibler personenbezogener Daten im Sinn von Art. 9 DS-GVO einschließt,
– nicht die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) einschließt und
– nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Der Verstoß gegen die Pflicht zur Bestellung ist bußgeldbewehrt (vgl. Art. 83 Abs. 4 lit. a DS-GVO).

Fazit

Auch Unternehmen, die keine Niederlassung in der EU haben, aber auf dem europäischen Markt tätig sind, müssen die DS-GVO voll anwenden. Darüber hinaus sind diese Unternehmen grundsätzlich verpflichtet, einen Vertreter in der EU zu benennen. Der europäische Gesetzgeber stellt die Aufsichtsbehörden mit Einführung des Marktortprinzips vor die nicht zu unterschätzende Herausforderung, den Geltungsanspruch der DS-GVO gegenüber Unternehmen in Drittstaaten durchzusetzen.

19.8
Kurzpapier Nr. 8

Maßnahmenplan „DS-GVO“ für Unternehmen

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.

Bedeutung

Die DS-GVO, die im Mai 2016 in Kraft getreten ist, wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Anders als die bisherige EU-Richtlinie wird diese EU-Verordnung ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und wird das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen. Gleichzeitig sieht das deutsche Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) eine ergänzende Neufassung des nationalen Rechts vor (z. B. BDSG-neu), soweit in der DS-GVO Spielraum für nationale Regelungen besteht. Viele Unternehmen sind aber noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die unabhängigen Datenschutzbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Information der Geschäftsleitung

Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet. In einem ersten Schritt ist daher von den betrieblichen Datenschutzbeauftragten und/oder den IT-Verantwortlichen die Geschäftsleitung zu informieren.

Start eines Projekts zur Umsetzung der DS-GVO

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind dahingehend zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DS-GVO gibt. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in einem Unternehmen. Da folglich verschiedene Personen bzw. Abteilungen im Unternehmen beteiligt sind, die untereinander koordiniert werden müssen, bietet es sich an, ein Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren. Die Kernaufgabe wird dabei sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

1. Bestandsaufnahme

Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell realisierten Rahmenbedingungen aller Datenverarbeitungen analysiert werden (Ist-Zustand). Dies betrifft u. a.

– die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden (bestehende Dokumentationen, bspw. ein Verfahrensverzeichnis, können hierfür einen Ausgangspunkt bilden),
– die dazugehörigen Rechtsgrundlagen (die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn entweder ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat),
– die Datenschutzorganisation (d. h. alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),
– die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
– die Dokumentation (z. B. Verfahrensverzeichnisse, Vorabkontrollen, Datenschutzkonzepte, IT-Sicherheitskonzepte, Sicherheitsvorfälle) und
– sofern vorhanden Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

2. Handlungsbedarf eruieren

Nunmehr ist der Soll-Zustand zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchzuführen. Dabei sind u. a. folgende Punkte vor dem Hintergrund der DS-GVO zu beachten (zu den einzelnen Themen erscheinen weitere Kurzpapiere):

– **Rechtsgrundlagen:**
  Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützt, ist zu prüfen, ob die Anforderungen des Art. 7 DS-GVO erfüllt sind (bei Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft ist zudem Art. 8 DS-GVO zu beachten).

– **Betroffenenrechte:**
  Den betroffenen Personen stehen umfangreiche Rechte zu, die der Verantwortliche zu beachten hat (z. B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS-GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).

– **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:**
  Die DS-GVO enthält spezifische Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Data Protection by design und Data Protection by default).

– **Dienstleistungsbeziehungen:**
  Dabei sollten insbesondere die bestehenden Verträge zur Auftragsverarbeitung überprüft werden. Die Art. 28 und 29 DS-GVO enthalten Vorgaben für Vereinbarungen mit Auftragsverarbeitern.

– **Dokumentationspflichten:**
  Die DS-GVO verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Zusätzlich sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z. B. für das Verarbeitungsverzeichnis in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 lit. a DS-GVO).

– **Datenschutz-Folgenabschätzung:**
  Die aus dem BDSG bekannte Vorabkontrolle wird durch die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO abgelöst und erfordert eine umfangreiche Dokumentation. Die Datenschutz-Folgenabschätzung kann zudem eine Konsultation der Aufsichtsbehörde nach sich ziehen (Art. 36 DS-GVO).

– **Meldepflichten:**
  Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO).

– **Datensicherheit:**
  Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten und die dafür implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).

– **Zertifizierung:**
  Schlussendlich besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

3. Umsetzung bis zum 25. Mai 2018

Bei der Umsetzung sind dann u. a. folgende Punkte wieder zu beachten:
– Anpassung der betroffenen Prozesse und Strukturen,
– Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt),
– Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten,
– Anpassung der Datenschutzorganisation,
– ggf. Bestellung eines Datenschutzbeauftragten,
– Reaktionsmechanismen auf Datenpannen,
– Organisation von Meldepflichten,
– Anpassung der Dienstleistungsbeziehungen,
– Aufbau der Dokumentation,
– Anpassung der IT-Sicherheit und
– ggf. Anpassung der Betriebsvereinbarungen.

19.9
Kurzpapier Nr. 9

Zertifizierung nach Art. 42 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.

Sinn und Zweck von Zertifizierungen

Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: *„Woher weiß man, ob datenschutzrechtliche Vorgaben von einem Unternehmen oder einer Behörde eingehalten werden?“.* Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifizierungen nachweisen zu lassen. Mit den Artikeln 42 und 43 der DS-GVO legt der Gesetzgeber einen rechtlichen Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Bisherige Erfahrungen der Aufsichtsbehörden

Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar, inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Förderung von Zertifizierungen

Einleitend weist Art. 42 Abs. 1 DS-GVO darauf hin, dass unter anderem auch die Aufsichtsbehörden auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegeln und -prüfzeichen fördern sollen. Diese dienen dazu, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bis es jedoch so weit ist, dass die Verordnung umgesetzt und angewandt werden kann, müssen die Mitgliedstaaten in einer engen Zusammenarbeit die in der DS-GVO geforderten Mechanismen und Kriterien entwickeln. Dies ist zeitlich, räumlich und kapazitiv eine große Herausforderung für alle Beteiligten.

Vorteile einer Zertifizierung

Die DS-GVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

– Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
– Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
– Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
– Sicherheit der Verarbeitung (Art. 32 Abs. 3)
– Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f)
– Datenschutz-Folgeabschätzung (ErwGr. 90)

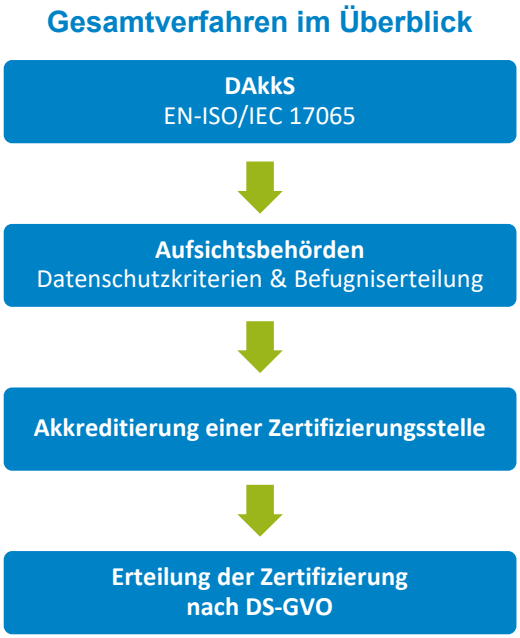
Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

Einhaltung der DS-GVO – auch mit Zertifikat

Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ebenso verdeutlicht Art. 42 Abs. 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Zertifizierungsstellen

Nach Art. 42 Abs. 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 Akkreditierung DSAnpUG („BDSG-neu“) vor. Die Kriterien für die Akkreditierung werden von den Aufsichtsbehörden entwickelt und beruhen u. a. auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der beiden Parteien in einem eigens dafür eingerichteten Ausschuss ist Voraussetzung für die Akkreditierung einer Zertifizierungsstelle. Erst danach und nach der Erteilung der Befugnis durch die zuständige Aufsichtsbehörde kann die Zertifizierungsstelle tätig werden. Sie darf im Anschluss, nach entsprechender Prüfung der Einhaltung der DS-GVO, Zertifizierungen erteilen.



Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss die zu zertifizierenden Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die bereits jetzt Informationssicherheit

leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen

Art. 42 Abs. 7 DS-GVO weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die bei Erfüllung der einschlägigen Voraussetzungen verlängert werden kann. Die zuständige Zertifizierungsstelle und die Aufsichtsbehörde können die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

Ausblick zu Datenschutz-Zertifizierungen

Zertifizierungen nach der DS-GVO bieten das Potenzial, künftig bei Verarbeitungsvorgängen (u. a. bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Cloud-Dienste entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einem bestimmten Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird. Ein Wildwuchs zahlreicher unterschiedlicher Zertifizierungsverfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.

19.10
Kurzpapier Nr. 10

Informationspflichten bei Dritt- und Direkterhebung

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.

Bedeutung der Informationspflichten

Die Informationspflichten bilden die Basis für die Ausübung der Betroffenenrechte (insbesondere der Art. 15 ff. DS-GVO). Nur wenn die betroffene Person weiß, dass personenbezogene Daten über sie verarbeitet werden, kann sie diese Rechte auch ausüben. Die Informationspflichten gemäß der DS-GVO gehen daher weit über die bisherige Rechtslage hinaus und müssen beachtet werden, sofern keine Ausnahmevorschriften greifen.

Die DS-GVO regelt die Informationsverpflichtungen des Verantwortlichen gegenüber der betroffenen Person in Abhängigkeit davon, ob personenbezogene Daten bei der betroffenen Person **(Direkterhebung**, Art. 13 DS-GVO) oder bei Dritten (**Dritterhebung**, Art. 14 DS-GVO) erhoben werden. Zu beachten ist, dass aus dieser Unterscheidung nicht pauschal abzuleiten ist, wer für die Information verantwortlich ist. Auch der Verantwortliche, der die Daten direkt bei der betroffenen Person erhoben hat, kann über Art. 13 DS-GVO hinaus zur Mitteilung nach Art. 14 Abs. 3 lit. c DS-GVO verpflichtet sein, wenn er die Daten gegenüber einem anderen Empfänger offenbaren möchte.

Informationspflichten bei Direkterhebung

Bei der Informationspflicht im Falle der **Direkterhebung** wird zwischen den Informationen unterschieden, die der betroffenen Person mitzuteilen sind (Art. 13 Abs. 1 DS-GVO) und solchen, die zur Verfügung zu stellen sind, um eine faire und transparente Verarbeitung der personenbezogenen Daten zu gewährleisten (Art. 13 Abs. 2 DS-GVO).

- Name (ggf. Firmenname gem. § 17 Abs. 1 HGB oder Vereinsname gem. § 57 BGB) und Kontaktdaten des Verantwortlichen sowie ggf. dessen Vertreter,
- Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten,
- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen und zusätzlich die Rechtsgrundlage, auf der die Verarbeitung fußt,
- das berechtigte Interesse, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten beruht (Art. 6 Abs. 1 lit. f DS-GVO),
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (vgl. Art. 4 Nr. 9 DS-GVO),
- Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln und zugleich Information, ob ein Angemessenheitsbeschluss der Kommission vorhanden ist oder nicht (bei Fehlen eines solchen Beschlusses ist auf geeignete oder angemessene Garantien zu verweisen und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind).

Zusätzlich sind nach Abs. 2 Informationen über

- die geplante Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,
- die Betroffenenrechte (Auskunfts-, Löschungs-, Einschränkungs- und Widerspruchsrechte sowie das Recht auf Datenübertragbarkeit),
- das Recht zum jederzeitigen Widerruf einer Einwilligung und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt,
- das Beschwerderecht bei einer Aufsichtsbehörde,
- ggf. die gesetzliche oder vertragliche Verpflichtung des Verantwortlichen, personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich Profiling) aussagekräftige Informationen über die verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung

zur Verfügung zu stellen.

Informationspflichten bei Dritterhebung

Auch im Falle einer **Dritterhebung** unterscheidet die DS-GVO zwischen mitzuteilenden Informationen (Art. 14 Abs. 1 DS-GVO) und zusätzlichen Informationen, die zur Gewährung einer

fairen und transparenten Verarbeitung zur Verfügung zu stellen sind (Art. 14 Abs. 2 DS-GVO).

Art und Inhalt der mitzuteilenden bzw. der zur Verfügung zu stellenden Informationen entsprechen in wesentlichen Teilen denjenigen, die auch im Falle einer Direkterhebung mitgeteilt werden müssen.

Allerdings hat die betroffene Person im Gegensatz zur Direkterhebung nicht an der Datenerhebung mitgewirkt und somit auch keine Kenntnis darüber, welche personenbezogene Daten erhoben wurden. Daher ist der Verantwortliche nach Art. 14 Abs. 1 lit. d DS-GVO verpflichtet, die Kategorien der verarbeiteten personenbezogenen Daten mitzuteilen. Diese Information muss so konkret sein, dass für den Betroffenen erkennbar wird, zu welchen Folgen die Verarbeitung führen kann. Nur dann kann er eine bewusste Entscheidung darüber treffen, ob er ergänzend von seinem Auskunftsrecht nach Art. 15 DS-GVO Gebrauch machen sollte.

Bei der Dritterhebung ist zudem nach Art. 14 Abs. 2 lit. f DS-GVO die Datenquelle anzugeben und, ob es sich dabei um eine öffentlich zugängliche Quelle handelt. Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig festgestellt werden, muss dennoch eine allgemeine Information gegeben werden.

Bei der Dritterhebung ist weiterhin zu beachten, dass Angaben über die berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DS-GVO) nicht – wie bei der Direkterhebung – unter Abs. 1 fallen, sondern im Rahmen der zusätzlichen Informationen nach Abs. 2 zur Verfügung gestellt werden müssen (Art. 14 Abs. 2 lit. b DS-GVO).

Zweckänderung und Übermittlung

Die Informationspflichten im Falle einer Zweckänderung gelten sowohl für die Direkterhebung als auch für die Dritterhebung. Neben der Information über die geänderte Zweckbestimmung sind alle Informationspflichten gemäß Art. 13 Abs. 2 DS-GVO (Direkterhebung) oder gemäß Art. 14 Abs. 2 DS-GVO (Dritterhebung) erneut zu erfüllen.

Die Übermittlung an einen Dritten ist häufig eine Zweckänderung, so dass schon aus diesem Grund vor der Übermittlung die betroffene Person entsprechend zu informieren ist. Darüber hinaus stellt Art. 14 Abs. 3 lit. c DS-GVO klar, dass bei der Offenlegung an einen neuen Empfänger (einschließlich Auftragsverarbeitern, vgl. Art. 4 Nr. 9 DS-GVO) informiert werden muss,

soweit dieser nicht von der bereits nach Art. 13 Abs. 1 lit. e DS-GVO erteilten Information über Empfänger oder Empfängerkategorien umfasst ist.

Zeitpunkt der Erfüllung der Informationspflichten

Bei der **Direkterhebung** müssen die Informationen zum Zeitpunkt der Erhebung der Daten mitgeteilt bzw. zur Verfügung gestellt werden.

Im Falle der **Dritterhebung** ist der Verantwortliche verpflichtet, die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitzuteilen (Art. 14 Abs. 3 DS-GVO). Diese Frist bestimmt sich nach den spezifischen Umständen, darf aber einen Monat nicht überschreiten. Die Monatsfrist ist eine Maximaldauer und sollte nicht pauschal angesetzt werden. Werden die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet, sind die Informationen spätestens zum Zeitpunkt der ersten Kontaktaufnahme mitzuteilen. Falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, müssen die Informationen spätestens zum Zeitpunkt der ersten Offenlegung erteilt werden.

Ausnahmen

Die Informationspflichten nach den Art. 13 und 14 DS-GVO bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Im Falle der Dritterhebung bestehen darüber hinaus keine Informationspflichten, wenn die Informationserteilung sich z. B. als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, die Daten einem Berufsgeheimnis unterliegen oder die Erlangung durch Rechtsvorschrift ausdrücklich geregelt ist.

Außerdem sind in den §§ 32 und 33 des neuen Bundesdatenschutzgesetzes (BDSG-neu) weitere Ausnahmen von den Informationspflichten normiert. Die Informationspflicht nach Art. 13 DS-GVO soll beispielsweise gem. § 32 Abs. 1 Nr. 4 BDSG-neu nicht bestehen, wenn die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Es bestehen jedoch Zweifel, ob die in den §§ 32 und 33 BDSG-neu vorgesehenen Beschränkungen der Informationspflichten nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in den §§ 32 und 33 BDSG-neu vorgesehene Beschränkung

der Informationspflichten aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Form der Informationspflicht

Gemäß Art. 12 Abs. 1 DS-GVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form (ggf. elektronisch) zur Verfügung zu stellen. Wird aber auf eine elektronisch verfügbare Information Bezug genommen, dann muss diese leicht auffindbar sein. Hierbei können auch Bildsymbole hilfreich sein.

Die leicht zugängliche Form bedeutet auch, dass die Informationen in der konkreten Situation verfügbar sein müssen. Sollen die Daten also von einer anwesenden Person erhoben werden, darf die Person in der Regel nicht auf Informationen im Internet verwiesen werden. Dies gilt gleichermaßen für eine schriftliche Korrespondenz auf dem Papierweg.

Nachweise der Informationspflichten

Der Verantwortliche hat im Hinblick auf das Transparenzgebot stets den Nachweis einer ordnungsgemäßen Erledigung der Informationspflichten zu erbringen (Art. 5 Abs. 1 lit. a und Abs. 2 DS-GVO).

Folgen eines Verstoßes

Der Verstoß gegen die Informationspflichten kann nach Art. 83 Abs. 5 lit. b DS-GVO mit einer Geldbuße bestraft werden.

Empfehlung

Es ist für Verantwortliche im eigenen Interesse ratsam, rechtzeitig die nach Art. 25 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen für eine zügige und korrekte Erfüllung der Informationspflichten zu treffen.

19.11
Kurzpapier Nr. 11

Recht auf Löschung/„Recht auf Vergessenwerden“

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.

Mit dem Inkrafttreten der DS-GVO erfährt die Löschung personenbezogener Daten gegenüber der bisherigen Rechtslage insofern eine Aufwertung, als die diesbezüglichen Bestimmungen detaillierter ausformuliert worden sind und zum Teil auch darüber hinausgehen. Das mit dem Löschungsanspruch der betroffenen Person verbundene „Recht auf Vergessenwerden“ wird zum ersten Mal ausdrücklich gesetzlich geregelt; es ergänzt die Löschung unmittelbar beim Verantwortlichen und die bereits bislang im BDSG verankerten Nachberichtspflichten.

Löschungspflicht

Wie aktuell in § 35 Abs. 2 BDSG-alt vorgesehen, bestimmt auch Art. 17 Abs. 1 DS-GVO, dass personenbezogene Daten auf Verlangen der betroffenen Person und/oder unter bestimmten Voraussetzungen ohne Verlangen der betroffenen Person eigenständig durch den Verantwortlichen unverzüglich gelöscht werden müssen. Art. 17 Abs. 1 DS-GVO benennt dazu folgende Fälle:

a) Die Notwendigkeit der Verarbeitung zur Zweckerreichung ist entfallen.
b) Die betroffene Person hat ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage.
c) Die betroffene Person legt gem. Art. 21 Abs. 1 oder 2 DS-GVO Widerspruch gegen die Verarbeitung ein; im Falle des Art. 21 Abs. 1 gilt dies nur, soweit keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen.
   Das Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO besteht ausschließlich bei Verarbeitungen, die auf Art. 6 Abs. 1 lit. e oder f DS-GVO gründen. Für die Löschungsverpflichtung bedarf es dabei einer Interessenabwägung.
   Anders bei Widersprüchen in Bezug auf Direktwerbung (Art. 21 Abs. 2 DS-GVO): Hier bedarf es keiner Interessenabwägung.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
e) Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

Der Verweis auf Art. 8 Abs. 1 DS-GVO (Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft) impliziert, dass die Daten rechtmäßig erhoben wurden. Eine Löschungspflicht ergibt sich damit allein aufgrund des Löschungsverlangens der betroffenen Person. Weil Diensten der Informationsgesellschaft (z. B. Soziale Netzwerke, Online-Spiele) in Bezug auf Minderjährige weniger Schutzbedarf als den betroffenen Personen zugestanden wird, bedarf es neben dem Löschungsverlangen keiner weiteren Voraussetzung; auch kann dieser Anspruch noch als Erwachsener geltend gemacht werden.

Recht auf Vergessenwerden

Das „Recht auf Vergessenwerden“ gemäß Art. 17 Abs. 2 DS-GVO bezieht sich, obwohl der Begriff im ErwGr. 65 als Synonym für „Löschung“ verwendet wird, auf die Tilgung (von Spuren) personenbezogener Daten, die durch Veröffentlichungen, insbesondere im Internet, einer breiten Öffentlichkeit zugänglich sind.

Der Verantwortliche, der die personenbezogenen Daten öffentlich gemacht hat und der gemäß Art. 17 Abs. 1 DS-GVO zu deren Löschung verpflichtet ist, hat unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, zu treffen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten (gleichfalls) verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Danach zieht der berechtigte Löschungsantrag einer betroffenen Person bzw. die bestehende Löschungspflicht eines Verantwortlichen dessen Pflicht nach sich, weitere Verantwortliche, die die zu löschenden Daten (noch) verarbeiten, über ein Verlangen des Betroffenen nach Löschung von Links, Kopien oder Replikationen zu informieren. Das Unterlassen entsprechender Bemühungen wird angesichts des Wortlauts der Norm und der fortlaufenden technischen Entwicklung nicht mit einem einfachen Verweis des Verantwortlichen auf unzumutbaren Aufwand begründet werden können.

Ausnahmen von der Löschungspflicht

Die Pflicht zur Löschung nach Art. 17 Abs. 1 und die Pflicht zur Information weiterer Verantwortlicher nach Art. 17 Abs. 2 DS-GVO entfallen, wenn gemäß Art. 17 Abs. 3 DS-GVO die Verarbeitung erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
b) zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt,
c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit,
d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DS-GVO, soweit die Löschung die Verwirklichung dieser Ziele ernsthaft beeinträchtigt,
e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Allerdings berechtigen die benannten Ausnahmen nicht zu einer zeitlich unbegrenzten Verarbeitung der jeweiligen personenbezogenen Daten. Auch diese Zwecke werden zu einem bestimmten Zeitpunkt erfüllt und die Verarbeitung der Daten wird zur Zweckerreichung nicht mehr erforderlich sein. Dann sind auch diese Daten zu löschen.

Nachberichtspflichten

Die bislang schon bestehenden Nachberichtspflichten zur Löschung (§ 35 Abs. 7 BDSG-alt) bleiben bestehen. Art. 19 DS-GVO verpflichtet den Verantwortlichen, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Löschung der personenbezogenen mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden.

Beschränkung des Löschungsanspruchs

Art. 23 DS-GVO befugt die Union und die Mitgliedstaaten, die Löschung gesetzlich zu beschränken, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet, eine notwendige und verhältnismäßige Maßnahme darstellt und (zumindest) einem der in Art. 23 Abs. 1 lit. a bis j DS-GVO genannten Zwecke dient. Hiervon hat der Bundesgesetzgeber in § 35 BDSG-neu Gebrauch gemacht: Im Fall nicht automatisierter Datenverarbeitung und unter den weiteren dort genannten Voraussetzungen ist statt des Löschungsanspruchs der betroffenen Person ein Anspruch auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO vorgesehen.

Anwendbarkeit der Regelungen des BDSG-neu

Es bestehen jedoch Zweifel, ob die in § 35 BDSG-neu vorgesehenen Beschränkungen des Rechts auf Löschung nach Art. 23 DS-GVO zulässig sind. Jedenfalls sind diese Regelungen grundsätzlich eng und im Sinne einer größtmöglichen Transparenz auszulegen. Ob und in welchem Umfang eine in § 35 BDSG-neu vorgesehene Beschränkung des Rechts auf Löschung aufgrund des Anwendungsvorrangs der DS-GVO tatsächlich angewendet werden kann, bleibt einer Entscheidung im jeweiligen konkreten Einzelfall vorbehalten.

Sanktionen

Bei Verstößen gegen die Löschungs- oder Nachberichtspflichten droht die Einleitung eines Bußgeldverfahrens (Art. 83 Abs. 5 lit. b DS-GVO).

19.12
Fragebogen für Unternehmen zur Vorbereitung auf die DS-GVO

Der Countdown läuft!

Ab dem 25. Mai 2018 muss jedes Unternehmen die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) und des neuen Bundesdatenschutzgesetzes (BDSG-neu) umgesetzt und in den Unternehmensalltag integriert haben. Bei Nichtbeachtung oder Verstößen sieht die neue Rechtslage einen drastisch erhöhten Bußgeldrahmen von bis zu 20 Millionen Euro vor.

Diese Neuerungen nehmen wir zum Anlass, Ihnen als kleinem oder mittelständischem Unternehmen Hilfestellung zur Umsetzung des neuen Datenschutzrechts zu geben. Mit den folgenden Fragen möchten wir Ihnen helfen, die Bereiche in Ihrem Unternehmen zu identifizieren, in denen Sie schon gut vorbereitet sind und die Bereiche, in denen es bis zum 25. Mai 2018 noch Handlungsbedarf für Sie gibt. Die Fragen geben Ihnen zugleich Anhaltspunkte, worauf wir bei zukünftigen Prüfungen besonderen Wert legen werden.

Fragen zur Vorbereitung auf die DS-GVO

1. Datenschutz ist Chefsache

a) Haben Sie sich als Geschäftsleitung schon mit den neuen Anforderungen der DS-GVO und des BDSG-neu befasst? Kennen Sie insbesondere die neuen Regelungen

- zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Art. 5 Absatz 2 DS-GVO)?
- zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten (Art. 12 bis 14 DS-GVO)?
- zu den Rechten der Betroffenen auf Datenübertragbarkeit (Art. 20 DS-GVO)?
- zu den technischen und organisatorischen Maßnahmen bei der Datenverarbeitung (Art. 25, 32 DS-GVO)?
- zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)?
- zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO)?

b) Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten bestellt (Art. 37 DS-GVO, § 38 BDSG-neu)?

c) Wurden Ihre Beschäftigten über die neuen Datenschutzregelungen informiert und/ oder geschult?

2. Bestandsaufnahme

a) Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten[5] verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)[6]? Denken Sie hierbei insbesondere an die

- Verarbeitung von Kundendaten
- Verarbeitung von Beschäftigtendaten
- Verarbeitung von Daten von Kindern
- Verarbeitung von Daten für Dritte als Auftragsverarbeiter

b) Wird dieses Verzeichnis regelmäßig aktualisiert? Wer ist hierfür in Ihrem Unternehmen zuständig?

[5] Personenbezogene Daten = alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (natürliche Person = Mensch, davon zu unterscheiden sind die juristischen Personen, wie z. B. GmbHs oder AGs), s. a. Art. 4 Nr. 1 DS-GVO.

[6] s. hierzu auch das Kurzpapier Nr. 1 der Aufsichtsbehörden – abzurufen unter www.datenschutz.hessen.de

3. Zulässigkeit der Verarbeitung

Auch nach neuem Recht benötigen Sie für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung oder eine Einwilligung der Betroffenen sein.

a) Haben Sie für alle Verarbeitungen (s. o. Nr. 2) eine Rechtsgrundlage nach der neuen Rechtslage (Art. 6 bis 11 DS-GVO sowie § 26 BDSG-neu)?

b) Haben Sie dies dokumentiert?

c) Haben Sie Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten usw. an die Anforderungen von Art. 7 und 13 DS-GVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?

4. Betroffenenrechte und Informationspflichten

a) Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DS-GVO).
Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher?

Besonders wichtig sind in diesem Zusammenhang folgende Informationen:

- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
- Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer
- Hinweis auf Betroffenenrechte
- Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Widerruf der Einwilligung
- Recht auf Beschwerde bei der Aufsichtsbehörde
- Herkunft der Daten

b) Wie stellen Sie die weiteren Betroffenenrechte (Art. 15 bis 22 DS-GVO) und deren technische Umsetzung sicher? Denken Sie dabei insbesondere an folgende Rechte:

- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf fristgemäße Löschung der verarbeiteten Daten
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

5. Personenbezogene Daten von Kindern

a) Verarbeiten Sie auch personenbezogene Daten von Kindern in Bezug auf Dienste der Informationsgesellschaft[7]?

b) Wenn ja, haben Sie in diesen Fällen an die besonderen Anforderungen an die Einwilligung gedacht (Art. 8 DS-GVO)?

6. Technischer Datenschutz

a) Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DS-GVO)? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung[8] dokumentiert?

b) Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? In welchen Fällen?

c) Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?

d) Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mitberücksichtigt werden (Art. 25 DS-GVO)?

7. Verträge prüfen

a) Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d. h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 26 bis 28 DS-GVO) angepasst?
Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

b) Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland[9] möglich ist[10], entsprechende zusätzliche Garantien/Vereinbarungen[11]?

- EU-Standardvertragsklauseln
- Binding Corporate Rules
- Privacy Shield (nur für die USA)

---

[7] Dienste der Informationsgesellschaft = jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung, z. B. Online-Verkauf von Waren, Video auf Abruf, Download eines Klingeltons, Beitritt zu sozialen Netzwerken.
[8] Schutzbedarfsklassifizierung = Bewertung des konkreten Schutzbedarfs der verarbeiteten Daten.
[9] Drittland = ein Land außerhalb der EU bzw. des europäischen Wirtschaftsraums.
[10] Eine Übermittlung liegt z. B. auch bei Supportzugriffen aus einem Drittland vor.
[11] s. hierzu auch das Kurzpapier Nr. 4 der Aufsichtsbehörden, abzurufen unter www.datenschutz.hessen.de

8. Datenschutz-Folgenabschätzung[12]

a) Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Art. 35 DS-GVO)? Dies gilt z. B. bei einer umfangreichen Verarbeitung besonderer Kategorien[13] personenbezogener Daten und insbesondere bei der Verwendung neuer Technologien.

b) Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?

c) Wer ist für diesen Prozess zuständig?

9. Meldepflichten

a) Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)?

- Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72 Stunden beachtet?
- Wer ist in Ihrem Unternehmen für die Meldung zuständig?

b. Falls Sie einen Datenschutzbeauftragten bestellt haben, denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde.

10. Dokumentation

a) Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen?

b) Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

[12] s. hierzu auch Kurzpapier Nr. 5 der Aufsichtsbehörden, abzurufen unter www.datenschutz.hessen.de

[13] Besondere Kategorien personenbezogener Daten = Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Sachwortverzeichnis zum 46. Tätigkeitsbericht

–	Schultagebuch	9.2
–	Spielersperrdatei	11.4
–	System-Konfigurationen	16.2
–	Terminpläne	7.5
–	Unternehmen Markt- und Meinungsforschung	7.7