Achtundvierzigster Tätigkeitsbericht zum Datenschutz
und
Zweiter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2019
gemäß Art. 59 der Verordnung (EU) Nr. 2016/679 i. V. m. § 15
des Hessischen Datenschutz- und Informationsfreiheitsgesetzes
sowie § 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

48. Tätigkeitsbericht zum Datenschutz / 2. Tätigkeitsbericht zur Informationsfreiheit

Beiträge zum Datenschutz und zur Informationsfreiheit
Herausgegeben vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit
Prof. Dr. Michael Ronellenfitsch
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Postfach 31 63, 65021 Wiesbaden

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

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

Inhaltsverzeichnis

Anhang I

Anhang II

Verzeichnis der Abkürzungen

a. a. O.	am angegebenen Ort
a. F.	alte Fassung
Abs.	Absatz
AG	Aktiengesellschaft
AI	Artificial Intelligence
AK Technik	Arbeitskreis Technik
Art.	Artikel
BAR	Bundesarbeitsgemeinschaft für Rehabilitation
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDSG	Bundesdatenschutzgesetz
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMG	Bundesmeldegesetz
BORA	Berufsordnung für Rechtsanwälte
BRAO	Bundesrechtsanwaltsordnung
BReg	Bundesregierung
BRDrucks.	Bundesratsdrucksache
bspw.	beispielsweise
BTDrucks.	Bundestagsdrucksache
BTHG	Bundesteilhabegesetz
BVerfSchG	Bundesverfassungsschutzgesetz
bzw.	beziehungsweise
ca.	circa
CVC	Card Value Code
d. h.	das heißt
DAkkS	Deutsche Akkreditierungsstelle
DIN	Deutsche Industrie-Norm(en)
DSFA	Datenschutzfolgenabschätzung
DS-GVO/DSGVO	Datenschutz-Grundverordnung

DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; kurz: Datenschutzkonferenz
e. V.	eingetragener Verein
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor (Europäischer Datenschutzbeauftragter)
EDSA	Europäischer Datenschutzausschuss
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
GG	Grundgesetz
ggf.	gegebenenfalls
GKI	Gemeinsame Kontrollinstanz
grds.	grundsätzlich
GVG	Gerichtsverfassungsgesetz
GWZ	Gebäude- und Wohnungszählung
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSB	Hessischer Datenschutzbeauftragter
HDSG	Hessisches Datenschutzgesetz
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HLBG	Hessisches Lehrerbildungsgesetz
HMDIS	Hessisches Ministerium des Innern und für Sport
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVSG	Hessisches Verfassungsschutzgesetz
HVGG	Hessisches Gesetz über das öffentliche Vermessungs- und Geoinformationswesen
HVwVfG	Hessisches Verwaltungs- und Verfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. R.	in der Regel
i. S. d.	im Sinne der/des

i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ID	Identifikation
IFK	Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder; kurz: Informationsfreiheitskonferenz
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
inkl.	inklusive
insb.	insbesondere
IT	Informationstechnik
ITZBund	Informationstechnikzentrum Bund
KI	Künstliche Intelligenz
KIS	Krankenhausinformationssystem
KMU	klein- oder mittelständiges Unternehmen
LfV	Landesamt für Verfassungsschutz
lit.	littera
LKA	Landeskriminalamt
LTDrucks.	Landtagsdrucksache
LUSD	Lehrer- und Schülerdatenbank
m. E.	meines Erachtens
MDK	Medizinischer Dienst der Krankenversicherung
o. a.	oben angegeben/angegebene/angegebener/angegebenes
o. g.	oben genannt/genannte/genannter/genanntes
OH	Orientierungshilfe
OwiG	Gesetz über Ordnungswidrigkeiten
PDF	Portable Document Format
Rdnr./Rn.	Randnummer
S.	Seite *oder* Satz
s.	siehe
s. a.	siehe auch
s. o.	siehe oben
s. u.	siehe unten

SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
sog.	sogenannte/sogenannter/sogenanntes
SSL	Secure Sockets Layer
StAnz.	Staatsanzeiger für das Land Hessen
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TOM	technisch-organisatorische Maßnahme
u. a.	unter anderem
u. Ä.	und Ähnliche/Ähnlicher/Ähnliches
u. U.	unter Umständen
UAG DSFA	Unterarbeitsgruppe Datenschutzfolgenabschätzung
US(A)	Vereinigte Staaten von Amerika
usw.	und so weiter
vgl.	vergleiche
VISZG	Gesetz über den Zugang von Polizei- und Strafverfolgungsbehörden sowie Nachrichtendiensten zum Visa Informationssystem (VIS-Zugangsgesetz)
VPN	Virtual Private Network
WP	Working Paper
z. B.	zum Beispiel
Ziff.	Ziffer

Register der Rechtsvorschriften*

*Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097)
BDSG a. F.	Bundesdatenschutzgesetz i. d. F. vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618) m. W. v. 09.11.2017, außer Kraft getreten am 25.05.2018 aufgrund Gesetzes vom 30.06.2017 (BGBl. I S. 2097)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084) zuletzt geändert durch Art. 1 Gesetz vom 22.11.2019
BORA	Berufsordnung für Rechtsanwälte in der Fassung vom 01.01.2020, zuletzt geändert durch Beschluss der Satzungsversammlung vom 06.05.2019, BRAK-Mitt. 2019, 245 f.
BRAO	Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 14 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2602)
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)
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466)
HBO	Hessische Bauordnung vom 28.05.2018 (GVBl. S. 198)
HDSG	Hessisches Datenschutzgesetz i. d. F. vom 07.01.1999 (GVBl. I S. 98), außer Kraft gesetzt am 25.05.2018 durch Gesetz vom 03.05.2018 (GVBl. S. 82)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 5 des Gesetzes vom 12.09.2018 (GVBl. S. 570)
HessStVollzG	Hessisches Strafvollzugsgesetz

HGB	Handelsgesetzbuch in der im BGBl Teil III, Gliederungsnummer 4100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2637)
HGO	Hessische Gemeindeordnung in der Fassung vom 7. März 2005 (GVBl. I S. 142), zuletzt geändert durch Art. 2 des Gesetzes zur Änderung des LandtagswahlG und anderer Vorschriften vom 30.10.2019 (GVBl. S. 310)
HHVG	Gesetz zur Stärkung der Heil- und Hilfsmittelversorgung (Heil- und Hilfsmittelversorgungsgesetz HHVG) vom 4. April 2017; (BGBl. I S. 778)
HLbG	Hessisches Lehrerbildungsgesetz vom 28. September 2011 (GVBl. 2011 S. 590)
HLbGDV	Verordnung zur Durchführung des Hessischen Lehrerbildungsgesetzes vom 28. September 2011 (GVBl. I S. 615), zuletzt geändert durch Artikel 6 des Gesetzes vom 24. März 2015 (GVBl. S. 118)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung i. d. F. vom 14.01.2005 (GVBl. I S. 14, geändert durch Gesetz vom 23.08.2018 (GVBl. S. 374)
HVGG	Hessisches Vermessungs- und Geoinformationsgesetz vom 03. Mai 2018 (GVBl. S. 82)
HWaldG	Hessisches Waldgesetz vom 27. Juni 2013 (GVBl. S. 458)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 09.12.2019 (BGBl. I S. 2146) m. W. v. 17.12.2019
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz) vom 18.06. 2009 (BGBl. I S. 1346)
RBStV	Rundfunkbeitragsstaatsvertrag vom 15. Dezember 2010, zuletzt geändert durch den Einundzwanzigsten Rundfunkänderungsstaatsvertrag, in Kraft getreten am 25. Mai 2018
SGB I	Das Erste Buch Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), zuletzt geändert durch Artikel 28 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2652)
SGB V	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Dezember 2019 (BGBl. I S. 2913)

SGB X	Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz, in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Artikel 9 des Gesetzes vom 14. Dezember 2019 (BGBl. I S. 2789)
SGB XII	Das Zwölfte Buch Sozialgesetzbuch – Sozialhilfe – (Artikel 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Artikel 11 des Gesetzes vom 14. Dezember 2019 (BGBl. I S. 2789)
SigG	Signaturgesetz i. d. F. vom 16.05.2001 (BGBl. I S. 876)
StVG	Straßenverkehrsgesetz vom 05.03 2003 (BGBl. I S. 310, berichtigt S. 919)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Artikel 15 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2652)
TKG	Telekommunikationsgesetz Gesetz vom 22.06.2004 (BGBl. I S. 1190), zuletzt geändert durch Gesetz vom 06.02.2020 (BGBl. I S. 146) m. W. v. 14.02.2020
TMG	Telemediengesetz vom 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Art. 11 des Gesetzes vom 11.07.2019 (BGBl. I S. 1066)
VVG	Versicherungsvertragsgesetzes vom 23.11.2007 (BGBl. I S. 2631)

Kernpunkte

1. Die DS-GVO verlangt einheitliches Vorgehen der Aufsichtsbehörden aller europäischen Ebenen und deren enge Zusammenarbeit. Meine Stabsstelle Europa fungiert dabei als Bindeglied für die Kommunikation auf Landes-, Bundes- und internationaler Ebene. Einen Einblick in die Tätigkeitsfelder liefert der Beitrag Ziff. I 3.2. Im Bereich der Technik ist der HBDI an der Erarbeitung einer Leitlinie zum Thema Blockchain in einer Expertengruppe des Europäischen Datenschutzausschusses beteiligt (Ziff. I 14.5). Ein einheitliches innerdeutsches Konzept zur Zumessung von Bußgeldern nach DS-GVO konnte von der Datenschutzkonferenz erarbeitet und veröffentlicht werden (Ziff. I 15.2 und Anhang I 3.1).
2. Weitere Resultate der Abstimmungsarbeit zur Vereinheitlichung der Durchsetzung der DS-GVO enthält mein diesjähriger Bericht zum Datenschutz im Anhang I Materialien. Da bis zum Erreichen tragbarer gemeinsamer Ergebnisse ein erheblicher Arbeitsaufwand meiner Mitarbeiterinnen und Mitarbeiter anfällt, soll darauf als weitere neue Tätigkeit des HBDI hingewiesen werden.
3. Die jährliche Überprüfung des Privacy Shields durch den Europäischen Datenschutzausschuss (EDSA) zeigt allmählich Fortschritte, wie z. B. die Besetzung des Amts der Ombudsperson. Allerdings sind nach wie vor viele Fragen in der praktischen Umsetzung offen (Ziff. I 3.1).
4. Seit Geltung der DS-GVO führt die Frage, ob und inwieweit eine Vereinbarung über eine Auftragsverarbeitung der Schriftform bedarf, zu Unsicherheiten bei den Anwendern. Der Beitrag Ziff. I 4.2 setzt sich mit den verschiedenen Rechtsansichten auseinander. Mit der Anpassung des Hessischen Datenverarbeitungsverbundsgesetz (DV-VerbundG) an die DS-GVO hat der hessische Gesetzgeber einen praktikablen Weg gefunden, die neuen Vorgaben hinsichtlich der Auftragsverarbeitung durch die HZD effektiv umzusetzen (Ziff. I 3.1).
5. Die zweckwidrige Verwendung personenbezogener Daten ist häufiger Beschwerdegegenstand. Ob im Bewerbungsverfahren (Ziff. I 4.4), bei Katasterauskünften an“ Dritte (Ziff. I 5.3), bei der Entsorgung von amtlichen Papieren und Unterlagen (Ziff. I 7.2) – stets war die Unkenntnis über den Geltungsbereich der Rechtsgrundlage oder Organisationsmängel Grund für die Datenschutzverletzung. Erheblich schwerer wiegt ein solcher Verstoß, wenn die Datenschutzverletzung trotz Kenntnis des Verbots zweckwidriger Verwendung erfolgte. Dies ist beim sogenannten Mitarbeiterexzess der Fall. In zwei Fällen führte private Neugier zur Verhängung eines Bußgelds (Ziff. I 15.1).

6. Datenschutzrechtlich tut sich im Bereich „Schule“ viel. Das Projekt Hessenbox ist abgeschlossen (Ziff. I 17.1). Das Hessische Schulportal entwickelt sich (Ziff. I 7.3). Der Einsatz von Office 365 im pädagogischen Bereich bleibt in der Prüfung (Ziff. I 7.4). Die Digitalisierung des Verfahrens der Schülerbeförderung ist datenschutzrechtlich zu prüfen (Ziff. I 7.5). Das Lehrerbildungsgesetz bedarf verbindlicher Datenverarbeitungsnormen (Ziff. I 7.1). Abgesehen von diesen Stichpunkten bleibt noch Vieles zu tun.
7. Im Gesundheitsbereich kam es zu ganz unterschiedlichen und teilweise ungewöhnlichen Fallkonstellationen, die mein Eingreifen erforderlich machten. So warf die Entsorgung von Altglas mit aufgeklebten Patientendaten einer Klinik Probleme auf (Ziff. I 9.2). In mehreren Fällen kam es durch eindringendes Wasser zu Schäden bei der Aufbewahrung von Patientendokumentationen (Ziff. I 9.3). Im frei zugänglichen „Service-Briefkasten“ einer Arztpraxis wurden auf Vertrauensbasis Rezepte und Überweisungen zur Abholung durch die betroffenen Patienten hinterlegt (Ziff. I 9.4). Eine Apotheke ging allzu freizügig mit Rezeptabholscheinen um (Ziff. I 9.6).
8. Das Thema Videoüberwachung erfasst mittlerweile in viele Lebensbereichen. Fälle aus dem Pflegedienst, der Gastronomie, dem Schwimmbadbetrieb, der privaten Grundstücksüberwachung und auch aus dem kommunalen Bereich zur Bekämpfung „wilden Mülls“ werden unter Ziff. I 10 exemplarisch dargestellt.
9. Internetdiensten und über das Internet zugreifbaren Websites ist es immanent, dass sie datenschutzrechtlich problematisch sein können. Die Nutzung von integrierten Tools, kleinen Diensten, Identifizierungs- und Authentifizierungsverfahren, Verschlüsselung der Kommunikation, Chat-Applikationen sowie die Einbindung von Schnittstellen zu Auftragsverarbeitern und die Datenhaltung sind häufige Schwachstellen (Ziff. 8.3, 13, 14, 15.3). Bei der Prüfung sogenannter Phishing-Attacken fiel auf, dass sowohl die im Vorfeld zur Abwehr als auch die zur Behebung nach Bekanntwerden ergriffenen Maßnahmen nicht den Anforderungen der DS-GVO genügen (Ziff. I 4.3). Das neue Handbuch 2.0 zum Standard-Datenschutzmodell unterstützt Verantwortliche, geeignete technisch-organisatorische Maßnahmen zum Datenschutz einzubinden (Ziff. I 14.4).
10. Vom Informationsfreiheitsgesetz wird allmählich, teilweise auch in Kommunen, Gebrauch gemacht. Die Bewährungsprobe des Gesetzes steht noch bevor.

Einleitung

War der 47. Tätigkeitsbericht zum Datenschutz durch die Darstellung der Maßnahmen zur Bewältigung der Umbruchsituation im Jahr 2018 geprägt, so begann im vorliegenden Berichtszeitraum die Konsolidierung der neuen Regelungen. Dies führte bei im Wesentlichen gleichbleibendem Arbeitsanfall zu einer Verlagerung des Schwerpunkts der Aufgabenwahrnehmung von der Beratungstätigkeit auf die Bearbeitung von Beschwerden. Angesichts des durch die Datenschutzreform veranlassten immensen innerorganisatorischen Mehraufwands (Ausschreibungsverfahren, Umverteilung von Diensträumen usw.) und wegen der – zwischenzeitlich behobenen – Unterbesetzung der Geschäftsstelle konnten die Bearbeitungsfristen für Beschwerden nicht immer eingehalten werden. Dies führte bereits zu Dienstaufsichtsbeschwerden, deren Bearbeitung ebenfalls Kapazitäten band. Es zeigte sich ferner, dass mit den vorhandenen personellen und sächlichen Mitteln die unionsrechtlich vorgesehene Kontrolltätigkeit vor allem im privaten Bereich nicht im gebotenen Maß durchführbar ist. Ob selbst bei Ausschöpfung aller Einsparmöglichkeiten die Vorgaben des Art. 52 Abs. 4 DS-GVO eingehalten werden kann, erscheint daher fraglich.

Auf die neuen Rechtsgrundlagen für die Tätigkeitsberichte wurde bereits im 47. Tätigkeitsbericht des HBDI hingewiesen. Dort wurde auch begründet, weshalb es zu den Aufgaben der Datenschutzaufsichtsbehörden zählt, ihre letztlich verfassungsrechtlich verankerte Sonderstellung als oberste Bundes- oder Landesbehörden zu konturieren. Dem dienen seit dem 35. Tätigkeitsbericht generelle Vorbemerkungen zum Stand des Datenschutzes und des Datenschutzrechts. Die aktuelle Diskussion ist geprägt durch die Erörterung von schon lange bekannten Positionen, die bereits Schlagwortcharakter angenommen hatten, aber erst jetzt virulent werden. Zu nennen ist hier die Künstliche Intelligenz (KI) und die Datensouveränität. Hier ist nicht der Ort für eine ausführliche Erörterung der genannten Themen. Aber gerade diese Themen bieten Anlass, sich mit der informationellen Selbstbestimmung als Fundament unseres Datenschutzrechts zu beschäftigen.

In Ergänzung hierzu zeigt mein zweiter Tätigkeitsbericht zur Informationsfreiheit auf, dass die Erstreckung des Rechts auf informationelle Selbstbestimmung in den Bereich des Informationszugangs zunehmend bei den Bürgerinnen und Bürgern sowie bei den öffentlichen Stellen angenommen wird.

So ist auch der gesetzlich angeordnete kommunale Satzungsvorbehalt für die Geltung der Informationsfreiheit (§ 81 Abs. 1 Nr. 7 HDSIG) bereits nach einem knappen Jahr der Geltung des Gesetzes von einigen Kommunen bereits in ein entsprechendes Informationszugangsrecht umgesetzt worden.

I
Erster Teil
48. Tätigkeitsbericht zum Datenschutz

1. Einführung

Die vom Bundesverfassungsgericht vorgenommene Ableitung eines Datenschutzgrundrechts aus der informationellen Selbstbestimmung (BVerfGE 65,1) wurde schon häufig, so auch in meinen früheren Tätigkeitsberichten, dargestellt. Im 1. Tätigkeitsbericht Informationsfreiheit, S. 197 ff. habe ich noch einmal die dogmatischen Grundlagen und die historische Entwicklung dieses Konstrukts des Bundesverfassungsgerichts skizziert. Es kann daher als bekannt vorausgesetzt werden, dass schon vor Erlass des Volkszählungsurteils die Bezeichnung und Konstruktion der informationellen Selbstbestimmung im Schrifttum kontrovers diskutiert worden war. Wem die Begriffsbildung zuzuschreiben ist (vgl. Steinmüller, Grundfragen des Datenschutzes, Gutachten erstattet im Auftrag des Bundesministers des Innern, BT-Drs. VI/3826 [1971], S.5 ff.; Christoph Mallmann, Datenschutz in Verwaltungs- und Informationssystemen: zur Verhältnismäßigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung, 1976), spielt letztlich keine Rolle mehr. Auch die Argumente der damaligen Mindermeinung sind überholt. Die Kritik an dieser Meinung ist dagegen immer noch aktuell. So sah Otto Mallmann die Gefahr, dass ein übertriebener Datenschutz Verwaltung und Wirtschaft paralysiere (Zum Stand der Datenschutzdiskussion, JZ 1973, 274). Das wird noch in der Gegenwart behauptet. Das Bundesverfassungsgericht ließ sich auf diesen Meinungsstreit nicht ein, sondern leitete die informationelle Selbstbestimmung eigenständig aus seiner früheren Rechtsprechung zum allgemeinen Persönlichkeitsrecht ab. Durch die Verknüpfung von Art. 1 Abs. 1 GG mit Art. 2 Abs.1 GG wurde das Abwägungsverbot im Einwirkungsbereich der Menschenwürde aufgehoben. Im Kernbereich der Menschenwürde blieb es jedoch bei der ausschließlichen Geltung des Art. 1 Abs.1 GG. Insofern bleibe ich trotz der Kritik von Bull (Informationelle Selbstbestimmung – Vision oder Illusion?, S.1) bei meiner Qualifizierung der informationellen Selbstbestimmung als rechtsstaatliche Fundamentalnorm. Das Verständnis des Datenschutzrechts als Abwägungsrecht macht es gegenüber einer Anwendung Künstlicher Intelligenz immun. Zugleich öffnet sich das Datenschutzrecht für die Berücksichtigung anderer Grundrechte als das allgemeine Persönlichkeitsrecht zur Bestärkung des Datenschutzes im Rahmen von Abwägungen. Die Zeit für eine Beschränkung des Datenschutzes auf den Schutz personenbezogener Daten ist abgelaufen. Auf der Ebene der EU hat man das erkannt. Der hessische Gesetzgeber hat hieraus ebenfalls erste Konsequenzen gezogen. Die Veranstaltungen aus Anlass des Inkrafttretens des Hessischen Datenschutzgesetzes vor 50 Jahren bieten Gelegenheit, die neuesten Entwicklungen im Zusammenspiel

von Datenschutz und Informationsfreiheit, Datensouveränität, Datenwirtschaft und Dateneigentum zu analysieren und zu würdigen.

2. Rechtsentwicklung und Gesetzgebung

2.1
DS-GVO – Eine Zwischenbilanz

Erste Erfahrungen im Umgang mit der DS-GVO veranlassten manche, sogleich eine Evaluation zu erarbeiten, die aber nach der bislang nur kurzen Geltungsdauer der DS-GVO nicht dazu dienen konnte, etwaige Vollzugsdefizite aufzudecken, sondern in Wahrheit die Wiederbelebung von Forderungen bezweckten, die im Gesetzgebungsverfahren nicht durchgesetzt werden konnten. Aufgabe des HBDI ist es aber lediglich, den Gesetzgeber auf neue Probleme des Datenschutzes hinzuweisen und ihn soweit zu beraten. Eine Korrektur der im Gesetzgebungsverfahren gefundenen Kompromisse zur Lösung überkommener Probleme steht dem HBSI nicht zu.

Mit der DS-GVO wurde über Grundsatzfragen eine Einigung erzielt, an der sich materiell nicht mehr rütteln lässt. Eine Fortschreibung der Reform bei ausdiskutierten Problembereichen wäre unzulässig. Eine Evaluation für den Normvollzug im Berichtszeitraum erfolgt daher nicht.

Im Hinblick auf die Rechtsentwicklung im Bund wird auf den Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Informationsfreiheit verwiesen.

Auf europäischer Ebene schritt die Regulierung des Verkehrs mit nichtpersonenbezogenen Daten voran. Insbesondere erlangte die Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union (ABl. L303 vom 28.11.2018, S. 59–68) im Berichtszeitraum Geltung. Personenbezogene Daten behandelt demgegenüber die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstige Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. 295 vom 21.11.2018, S. 39–98).

2.2
Änderung des DV-Verbundgesetzes

Die Hessische Zentrale für Datenverarbeitung (HZD) verarbeitet auch personenbezogene Daten im Auftrag hessischer Dienststellen. Mit der Ergänzung des Datenverarbeitungsverbundgesetzes (DV-Verbundgesetz) wird als Ersatz für die jeweils erforderlichen, einzeln abzuschließenden Auftragsverträge ein

anderes Rechtsinstrument i. S. d. Art. 28 Abs.3 DS-GVO geschaffen, das eine effektivere Verfahrensweise bei der Auftragserteilung zulässt.

Die Hessische Zentrale für Datenverarbeitung (HZD) ist gem. § 1 Abs. 1 DV-Verbundgesetz der zentrale Dienstleister für die Hessische Landesverwaltung. Rechtlich ist diese Dienstleistung als Auftragsverarbeitung i. S. d. Art. 28 DS-GVO anzusehen. Das bedeutet, dass für jede Dienstleistung, die die HZD als Auftragsverarbeiter für eine Dienststelle als Verantwortlichen erbringt, ein Vertrag nach Art. 28 Abs. 1 DS-GVO abzuschließen wäre. Dies hätte einen immensen Verwaltungsaufwand erfordert. Deshalb wurde nach einer Möglichkeit gesucht, die Anforderungen der Grundverordnung zu erfüllen, den Verwaltungsaufwand aber zu reduzieren.

Ich habe der Landesregierung deshalb vorgeschlagen, das DV-Verbundgesetz so zu erweitern, dass Einzelverträge nicht mehr erforderlich sind.

Die Landesregierung hat diesen Vorschlag aufgegriffen und folgenden Regelungsvorschlag dem Parlament unterbreitet:

§ 1 Abs. 2 DV-VerbundG wird wie folgt gefasst:

„Die Hessische Zentrale für Datenverarbeitung kann durch die Landesregierung oder die jeweils zuständige Landesbehörde bei zentralen oder sonstigen gemeinsamen Verfahren beauftragt werden, verbindlich für alle beteiligten Stellen des Landes den Betrieb des Verfahrens zur automatisierten Datenverarbeitung als Auftragnehmerin im Sinne des Art. 28 der Verordnung (EU) Nr. 202016/679 des Europäischen Parlaments und des Rates vom 27. April 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 Nr. L 119 S.1, Nr. L 314 S. 72, 2018 Nr. L 127 S. 2) und des § 57 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom 3. Mai 2018 (GVBl. S. 82), geändert durch Gesetz vom 12. September 2018 (GVBl. S. 570), durchzuführen. Zur Erfüllung der nach diesem Gesetz vorgesehenen Aufgaben unterhält und pflegt sie ein auf das jeweilige Verfahren abgestimmtes Betriebshandbuch, aus dem sich die nach Art. 28 Datenschutz-Grundverordnung erforderlichen Garantien, Rechte und Pflichten eines Auftragsverarbeiters ergeben.“

Der Hessische Landtag hat das Gesetz am 11.12.2019 in zweiter Lesung unverändert beschlossen.

Es wird meine Aufgabe sein, regelmäßig zu überprüfen, ob das von der HZD nach dieser Vorschrift zu führende Betriebshandbuch den Anforderungen, die an Einzelverträge zu stellen wären, genügt.

3. Europa, Internationales

3.1
Internationale Datentransfers – 3. Jährliche Überprüfung des Privacy Shield

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

Über die beiden Überprüfungen der Vorjahre wurde bereits berichtet (vgl. 46. TB, Ziff. 4.1 und 47. TB, Ziff. 4.2.1). Im vorliegenden Berichtsjahr fand die Überprüfung wieder in Washington D.C. statt. Die etwa 40-köpfige Delegation aus den USA wurde von Handelsminister Wilbur Ross angeführt. Die europäische Delegation setzte sich aus acht Vertretern der europäischen Datenschutz-Aufsichtsbehörden und Vertretern der Europäischen Kommission zusammen.

Wie schon bei der Überprüfung im letzten Jahr (47. TB, Ziff. 4.2.1, S. 94 f.) umfasste die Prüfung zum einen Fragen nach der praktischen Umsetzung des Privacy Shield. Hier lag der Fokus vor allem auf Ablauf und Inhalt des (Re-)Zertifizierungsprozesses und den Mechanismen, mit denen sichergestellt werden soll, dass die zertifizierten Unternehmen die Bedingungen auch tatsächlich erfüllen und zum Beispiel gewährleisten, dass Betroffene die ihnen nach dem Privacy Shield zustehenden Rechte auch tatsächlich ausüben können.

Seinen Bericht zur dritten jährlichen Überprüfung des Privacy Shield hat der Europäische Datenschutzausschuss (EDSA) unter https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en veröffentlicht. Es konnte insgesamt festgestellt werden, dass das US-Handelsministeriums und die Federal Trade Commission weiterhin bemüht sind, die im EU-US Privacy Shield gemachten Zusagen umzusetzen.

Auch im diesjährigen Bericht werden jedoch Bereiche benannt, in denen weitere Arbeit nötig ist: Größter Kritikpunkt bleibt die Sorge, dass die Aufsicht über die zertifizierten Organisationen eher auf formale Aspekte beschränkt sein könnte und zu wenig substanzielle Kontrollen stattfinden. Ein weiterer Punkt, der nach wie vor näherer Betrachtung bedarf, sind die Weiterüber-

mittlungen von Privacy Shield-zertifizierten Unternehmen an Dritte bzw. in weitere Drittstaaten. Hier muss aus Sicht des EDSA sichergestellt werden, dass die im Privacy Shield hierzu festgelegten Bedingungen in der Realität auch eingehalten werden, damit der Privacy Shield nicht zum Schlupfloch für unkontrollierte Weiterübermittlungen der Daten an nicht zertifizierte Organisationen innerhalb der USA oder Empfänger in einem weiteren Drittstaat ohne angemessenes Datenschutzniveau genutzt werden kann. Schließlich sollen auch weiterhin der Bereich der Beschäftigtendaten und der Rezertifizierungsprozess im Auge behalten werden.

Neben den praktischen Umsetzungsfragen nahm wieder die Frage nach staatlichen Zugriffen auf Daten, die unter dem Privacy Shield in die USA transferiert wurden, einen großen Raum ein. Auch hier kann festgehalten werden, dass einige Schlussfolgerungen des Europäischen Datenschutzausschusses aus dem vergangenen Jahr von den US-Behörden aufgegriffen wurden. So wurde inzwischen das Amt der Ombudsperson, das durch den EU-US Privacy Shield überhaupt erst geschaffen wurde, fest besetzt. Auch ist der Privacy and Civil Liberties Oversight Board nun wieder vollständig besetzt. Aufgabe dieses Gremiums ist es, darauf zu achten, dass die US-Behörden bei ihren Bemühungen zur Terrorismusbekämpfung auch die Privatsphäre und bürgerliche Freiheiten angemessen berücksichtigen.

Insgesamt gilt weiterhin, dass das Gebiet der internationalen Datentransfers mit gravierenden Unsicherheiten belastet ist. Nach wie vor sind Verfahren vor dem EuGH anhängig, deren Ausgang weitreichende Bedeutung für die Zulässigkeit von Datentransfers in Staaten außerhalb der EU haben wird. Im ersten Quartal 2020 ist im Verfahren C-311/18 Facebook Ireland und Schrems (Schrems II) mit einer Entscheidung des EuGH zu rechnen, die Einfluss auf internationale Datentransfers und die dafür zur Verfügung stehenden Instrumente nach Kapitel V der DS-GVO haben wird.

3.2
Europaweite Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden nach der Datenschutz-Grundverordnung (s. a. 47. Tätigkeitsbericht, Ziff. 4.2.2)

Mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) haben sich, wie bereits im 47. Tätigkeitsbericht geschildert, zahlreiche Neuerungen für die Zusammenarbeit der Aufsichtsbehörden in Deutschland und Europa ergeben. Aufgrund der neuen europarechtlichen Vorgaben war im Berichtszeitraum eine deutliche Intensivierung der Zusammenarbeit und ein Anstieg des Prüfungsaufwandes zu beobachten. Die beim HBDI im vergangenen Jahr neu eingerichtete Stabsstelle Europa und Internationales fungiert als

Bindeglied für die Kommunikation zwischen dem HBDI und verschiedenen Stellen außerhalb Hessens in Deutschland, Europa und der Welt.

Durch die DS-GVO wurden die Aufsichtsbehörden in Fällen grenzüberschreitender Verarbeitungen personenbezogener Daten zu einer engeren Zusammenarbeit verpflichtet. Eine grenzüberschreitende Verarbeitung liegt gemäß Art. 4 Nr. 23 DS-GVO vor, wenn eine Verarbeitung im Rahmen der Tätigkeit von Niederlassungen des Verantwortlichen bzw. Auftragsverarbeiters in mehr als einem Mitgliedstaat erfolgt oder wenn die Verarbeitung im Rahmen der Tätigkeit einer einzelnen Niederlassung eines Verantwortlichen bzw. Auftragsverarbeiters in der EU erfolgt, aber erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Der sog. One-Stop-Shop

Nach dem neu eingeführten Konzept des sog. One-Stop-Shop ist eine Aufsichtsbehörde (i. d. R. die Aufsichtsbehörde der sog. Hauptniederlassung des Verantwortlichen bzw. Auftragsverarbeiters, Art. 56 Abs. 1 DS-GVO) als sog. federführende Aufsichtsbehörde einziger Ansprechpartner des Verantwortlichen bzw. Auftragsverarbeiters nach Art. 56 Abs. 6 DS-GVO, d. h. ein Unternehmen muss sich wegen ein und derselben Datenverarbeitung nur mit einer Aufsichtsbehörde auseinandersetzen. Dies bedeutet aber nicht, dass die federführende Aufsichtsbehörde allein entscheidet. Vielmehr wirken neben der federführenden Aufsichtsbehörde auch alle betroffenen Aufsichtsbehörden an der Entscheidungsfindung mit. „Betroffen“ sind nach Art. 4 Nr. 22 DS-GVO alle Aufsichtsbehörden der Mitgliedstaaten, in deren Hoheitsgebiet der Verantwortliche bzw. Auftragsverarbeiter niedergelassen ist, betroffene Personen ihren Wohnsitz haben oder bei denen eine Beschwerde eingereicht wurde. Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden arbeiten im Kooperationsverfahren gemeinsam und versuchen, einen Konsens zu erzielen (Art. 60 Abs. 1 DS-GVO). Nach Prüfung des Falles legt die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Beschlussentwurf vor (Art. 60 Abs. 3 Satz 2 DS-GVO), gegen den die betroffenen Aufsichtsbehörden bei Bedarf Einspruch einlegen können (Art. 60 Abs. 4 DS-GVO). Bei Meinungsverschiedenheiten wird die Angelegenheit dem Europäischen Datenschutzausschuss (EDSA) im Kohärenzverfahren nach Art. 63 DS-GVO zur verbindlichen Entscheidung vorgelegt.

Neue Formen der Zusammenarbeit: Amtshilfe und gemeinsame Maßnahmen

Neben dem allgemeinen Gedanken des One-Stop-Shop sieht die DS-GVO mit der gegenseitigen Amtshilfe (Art. 61 DS-GVO) und sog. gemeinsamen Maßnahmen (Art. 62 DS-GVO) weitere Möglichkeiten der Zusammenarbeit vor. Erste Erfahrungen haben nun gezeigt, dass insbesondere von Amtshilfeersuchen im Rahmen der Fallbearbeitung und zum Informationsaustausch reger Gebrauch gemacht wird. So hat der HBDI im Berichtszeitraum 28 Amtshilfeersuchen anderer europäischer Aufsichtsbehörden bearbeitet und neun Amtshilfeersuchen an andere Aufsichtsbehörden gestellt.

Die neuen Verfahrensregelungen dienen insgesamt dazu, bei grenzüberschreitenden Datenverarbeitungen eine möglichst europaweit einheitliche Auslegung und Anwendung der DS-GVO zu erzielen. Darüber hinaus soll die Kommunikation mit den Aufsichtsbehörden sowohl für Verantwortliche und Auftragsverarbeiter als auch für betroffene Personen vereinfacht werden.

Beispiel „Binding Corporate Rules“

Ein anschauliches Beispiel für die verstärkte Zusammenarbeit der Aufsichtsbehörden unter der DS-GVO stellt das geänderte Genehmigungsverfahren von Binding Corporate Rules (deutsch: verbindliche interne Datenschutzvorschriften; kurz: BCR) dar. BCR sind Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich eine Unternehmensgruppe oder Gruppe von Unternehmen verpflichtet, um personenbezogene Daten innerhalb der Unternehmensgruppe in sog. Drittländer (d. h. Länder außerhalb des Europäischen Wirtschaftsraumes) zu übermitteln, die an und für sich kein angemessenes Datenschutzniveau bieten. Auf diese Weise soll ein konzernweit einheitliches Datenschutzniveau hergestellt werden, das die hohen Standards der DS-GVO widerspiegelt.

BCR werden in einem europaweiten Kooperationsverfahren, d. h. von Aufsichtsbehörden mehrerer Mitgliedstaaten gemeinsam geprüft. Hierbei agiert eine Aufsichtsbehörde als Federführung bzw. sog. BCR Lead und koordiniert das Verfahren. Eine oder zwei weitere Aufsichtsbehörden werden unterstützend als sog. Co-Prüfer tätig. Zudem müssen alle europäischen Aufsichtsbehörden gemäß dem in Art. 63 DS-GVO festgelegten Konsistenzmechanismus einbezogen werden und Gelegenheit zur Prüfung und Kommentierung der BCR erhalten.

Während unter der früheren Datenschutz-Richtlinie noch ein Verfahren der gegenseitigen Anerkennung („Mutual Recognition“) stattfand, muss nun der EDSA eine Stellungnahme zu den BCR abgeben. Erst wenn diese positiv

ausfällt, kann eine Genehmigung durch den BCR Lead erfolgen, die dann für alle anderen Aufsichtsbehörden bindend ist. Alle europäischen Aufsichtsbehörden werden damit stärker in die Verantwortung bzw. Pflicht genommen. Das Ziel der Verfahrensneuerung ist eine stärkere Vereinheitlichung der BCR, womit aber auch ein neuer und erhöhter Prüfungsaufwand für die Aufsichtsbehörden einhergeht.

Derzeit sind über 125 Anträge auf Genehmigung von BCR anhängig. Für acht dieser BCR-Verfahren ist der HBDI europaweit als sog. BCR Lead federführend zuständig. In 17 BCR-Verfahren hat der HBDI die Federführung innerhalb Deutschlands und in drei Verfahren zugleich die Co-Prüfung übernommen. Darüber hinaus müssen Unternehmen, deren BCR vom HBDI noch unter der früheren Datenschutz-Richtlinie genehmigt wurden, diese aktualisieren, an die Anforderungen der DS-GVO anpassen und dem HBDI zur Prüfung vorlegen.

Fallbearbeitung im „IMI-System“

Neben den BCR-Verfahren werden in der Stabsstelle Europa und Internationales beim HBDI auch alle anderen Verfahren bearbeitet, die eine Zusammenarbeit mit anderen deutschen und europäischen Aufsichtsbehörden erforderlich machen. Um die geforderte Zusammenarbeit elektronisch zu ermöglichen und zu erleichtern, wird unter anderem das IMI-System (Internal Market Information System, deutsch: Binnenmarkt-Informationssystem) eingesetzt. Im Berichtszeitraum waren vom HBDI (Stand: 29.11.2019) insgesamt 910 in IMI eingetragene Fälle in der neuen Form der europäischen Zusammenarbeit zu bearbeiten. In 244 dieser Fälle hat sich der HBDI als „betroffen“ gemeldet und ist daher an der Bearbeitung beteiligt. In weiteren sieben Fällen hat der HBDI die Federführung übernommen. Fast alle diese Fälle wären dem HBDI vor der Geltung der DS-GVO entweder gar nicht zur Kenntnis gelangt oder direkt an die „zuständige“ Aufsichtsbehörde verwiesen worden, in deren Aufsichtsbereich der Verantwortliche bzw. Auftragsverarbeiter, gegen den sich die Beschwerde richtet, seinen Sitz hat.

Zusätzliches Novum: Englischsprachigkeit der Arbeit

Ein zusätzliches Novum für die Arbeit des HBDI in Fällen, die nach der DS-GVO nun mit anderen Aufsichtsbehörden in Europa bearbeitet und abgestimmt werden müssen, ist die fast ausschließliche Englischsprachigkeit der Arbeit. So erfolgt etwa der Schriftverkehr mit den europäischen Gremien oder anderen europäischen Aufsichtsbehörden in englischer Sprache und die offizielle Sprache der Kooperationsverfahren und Beschwerdebearbeitung im IMI-System ist Englisch. Beim HBDI in deutscher Sprache eingegangene

Beschwerden sowie die gesamte Kommunikation mit dem Verantwortlichen bzw. Auftragsverarbeiter müssen daher in Fällen grenzüberschreitender Verarbeitungen übersetzt werden. Zudem ergeben sich im Rahmen der Zusammenarbeit mit den europäischen Aufsichtsbehörden relativ enge gesetzliche Fristen, die die Behörden in Wahrnehmung ihrer Aufgaben einzuhalten haben.

Fazit

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

4. Querschnitt

4.1 Änderung bei der Verpflichtung zur Benennung eines Datenschutzbeauftragten und die Auswirkungen

Die Verpflichtung zur Benennung eines Datenschutzbeauftragten wurde durch das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU zum 26.11.2019 geändert.
Ergänzend zu den unverändert fortbestehenden Voraussetzungen ist nunmehr erst dann ein Datenschutzbeauftragter zu benennen, wenn ein Verantwortlicher oder Auftragsverarbeiter in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Der neue § 38 Abs. 1 Satz 1 BDSG lautet nunmehr:

> *§ 38 BDSG*
> *(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.*

Bei Ermittlung der Personenanzahl sind neben den (freien) Mitarbeitern in Voll- und Teilzeit auch die Geschäftsführer, Vorstandsmitglieder, Ärzte, Apotheker, Steuerberater, Versicherungsvermittler usw. zu berücksichtigen.

Mit der Anhebung der maßgeblichen Personenzahl in § 38 Abs. 1 Satz 1 BDSG sollte vor allem eine Entlastung kleinerer und mittlerer Unternehmen sowie ehrenamtlich tätiger Vereine und Praxen erreicht werden.

Auch wenn der Gesetzgeber diese entlasten will, gibt es keinen Grund zur Entwarnung im Datenschutzrecht. Denn die Vorgaben zum Datenschutz und zur IT-Sicherheit gelten auch für diese weiter – egal, ob ein Datenschutzbeauftragter benannt werden muss oder nicht. Einer verantwortlichen Stelle oder einem Auftragsverarbeiter steht jedoch die freiwillige Benennung eines Datenschutzbeauftragten gemäß Art. 37 Abs. 4 Satz 1, 1. Alternative DS-GVO frei, um die datenschutzrechtlichen Vorgaben im erforderlichen Maße umzusetzen.

Die Abberufung interner Datenschutzbeauftragter aufgrund der gesetzlichen Änderung (Wegfall der Benennungspflicht) halte ich für zulässig. Allerdings können sich hier arbeits- bzw. zivilrechtliche Folgefragen ergeben. Wie sich die zuständigen Gerichte positionieren, bleibt abzuwarten.

4.2
Schriftformerfordernis bei Vereinbarungen über Auftragsverarbeitung

Seit Geltung der Datenschutz-Grundverordnung (DS-GVO) wurde ich oft gefragt, ob nach der neuen Rechtslage die Vereinbarung über Auftragsverarbeitung einer Schriftform bedürfe.

Bis zum 25. Mai 2018 kam als elektronischer Ersatz für die durch § 11 Abs. 2 Satz 2 BDSG a. F. für Auftragsdatenverarbeitungsverträge vorgeschriebene Schriftform nur ein elektronisches Dokument in Frage, das den Namen des Erklärenden enthielt und mit einer qualifizierten elektronischen Signatur nach § 2 Nr. 3 Gesetz über Rahmenbedingungen für elektronisch Signatur (SigG) versehen war (§ 126 a BGB).

Ob die seit 25. Mai 2018 geltende DS-GVO auch andere elektronische Formen für Vereinbarungen über Auftragsdatenverarbeitung zulässt, ist dem Wortlaut des Art. 28 Abs. 9 nicht eindeutig zu entnehmen. Der Auftragsverarbeitungsvertrag oder ein anderes Rechtsinstrument (z. B. eine rechtsverbindliche Verpflichtungserklärung des Auftragsverarbeiters) sind nach dieser Regelung schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

Das Schriftformerfordernis des Art. 28 Abs. 9 DS-GVO ist nicht identisch mit der Schriftform nach § 126 BGB. Es muss demnach nicht wie nach § 126 Abs. 1 BGB zwingend eine vom Aussteller eigenhändig unterschriebene Urkunde erstellt werden. Von den Funktionen der BGB-Formvorschrift, Warnfunktion, Beweisfunktion mit Identitäts-, Echtheits- und Verifikationsfunktion, Informationsfunktion (Palandt/Ellenberger § 125 Rdnr. 2 ff) verfolgt es lediglich den letztgenannten Zweck. Dass die Vertragspartner nicht vor unüberlegten oder übereilten Bindungen geschützt werden müssen, ist offensichtlich, denn Auftragsverarbeitungsverhältnisse werden nicht spontan eingegangen, sondern sind das Ergebnis von Verhandlungs- und Auswahlprozessen. Es sind auch kaum Situationen zu erwarten, in denen der Inhalt des Auftrags, die Identität der Vertragsparteien oder die Echtheit der Vereinbarungen bewiesen werden müssten. Dies dürfte erst recht gelten, wenn die Kommission und die Aufsichtsbehörden künftig Standardvertragsklauseln entwickelt haben sollten (Art. 28 Abs. 7 und 8 DS-GVO) und die Vertragsparteien wie zu erwarten in der Regel diese verwenden werden. Mit der in der DS-GVO angeordneten Schriftform soll sichergestellt werden, dass die Beteiligten die Möglichkeit haben, sich dauerhaft und zuverlässig über den Inhalt des Auftragsverarbeitungsvertrages oder einer einseitigen Verpflichtungserklärung zu informieren.

Diese dauerhafte Informationsfunktion erfüllt auch die Textform, wie sie in § 126b BGB geregelt ist (Palandt, a. a. O.).

Der Austausch von Computerfaxe oder E-Mails mit oder ohne PDF-Anhang genügt daher dem Schriftformerfordernis des Art. 28 Abs. 9 DS-GVO. Der Auftragsverarbeiter könnte auch einen Vertragstext auf seiner Webseite einstellen und der Verantwortliche die Annahmeerklärung durch Anklicken eines Kästchens wirksam abgeben (vgl. entsprechend für die Abgabe einer Einwilligungserklärung EG. 32 DS-GVO). In diesem Fall müsste sichergestellt sein, dass der Verantwortliche den Vertrag speichern und ausdrucken kann. Die DS-GVO verlangt nicht, dass ein Download tatsächlich erfolgt. Anders dagegen die Textform nach § 126 b BGB, sie ist bei Erklärungen auf Webseiten nur gewahrt, wenn der Empfänger die Erklärung ausdruckt oder auf einem Datenträger speichert. So mangelt es nach Auffassung des BGH (NJW 2010, 3566, 3567 Rdnr. 19) bei Widerrufsbelehrung auf einer Webseite an der notwendigen Textform, wenn der Empfänger die Seite nicht herunterlädt oder ausdruckt.

Die systematische Betrachtung der DS-GVO stützt ebenfalls die Auffassung, dass mit „elektronischem Format“ in Art. 28 Abs. 9 nicht ein nach § 126 a BGB elektronisch signiertes Dokument gemeint sein kann. In Art. 30 Abs. 3 DS-GVO findet sich für das Führen des Verarbeitungsverzeichnisses eine wortgleiche Schriftformregelung. Es ist jedoch kein Grund ersichtlich, weshalb ein Verzeichnis von Verarbeitungstätigkeiten mit einer qualifizierten elektronischen Signatur versehen werden sollte. Es gibt aber auch keine Anhaltspunkte, dass der Unionsgesetzgeber den Begriff „elektronisches Format“ in den beiden Regelungen mit unterschiedlichem Inhalt verwendet hat.

Auch in der Literatur wird ganz überwiegend die Ansicht vertreten, dass das von Art. 28 Abs. 9 DS-GVO als Schriftform zugelassene elektronische Format keine qualifizierte elektronische Signatur nach deutschen Recht erfordert, sondern damit eine im Verhältnis zu § 126 b BGB sogar noch etwas großzügigere Textform gemeint ist. (J. Hoffmann in A. Roßnagel, Europäische Datenschutz-Grundverordnung, S. 180 (Textform), J. Albrecht / F. Jotzo, Das neue Datenschutzrecht der EU, S. 98 (Textform), P. Laue u. a., Das neue Datenschutzrecht in der betrieblichen Praxis, S. 167, K-U. Plath, BDSG/DS-GVO, Art. 29, Rdnr. 17, C. Piltz, Die Datenschutz-Grundverordnung, K&R, 2016, S. 709, 713, a. A. Martini in Paal/Pauly, Datenschutz-Grundverordnung, Art. 28, Rdnr. 75).

Die geringeren Anforderungen an die Schriftform können sich unter Umständen zwar nachteilig auswirken. Wird der Auftragsverarbeitungsvertrag z. B. lediglich durch korrespondierende E-Mails begründet, kann es bei späteren Differenzen über die Vereinbarung zu Beweisrisiken kommen. Die DS-GVO

überlässt es trotzdem den Parteien, zu entscheiden, wie beweissicher sie Abschluss und Inhalt des Auftragsverarbeitungsvertrages dokumentieren möchten.

4.3
Datenschutz im Umgang mit Phishing-Vorfällen

Seit Einführung der Meldepflicht von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde erreichen mich vermehrt Verletzungsmeldungen, die die erfolgreiche Durchführung sogenannter Phishing-Attacken zum Gegenstand haben. Bei der Prüfung dieser Vorfälle fällt häufig auf, dass sowohl die im Vorfeld zur Abwehr als auch die zur Behebung nach Bekanntwerden ergriffenen Maßnahmen nicht den Anforderungen der DS-GVO genügen.

Ziel von sogenannten Phishing-Angriffen ist das Ausspähen von Zugangsdaten (z. B. Benutzername und Passwort). Um dies zu erreichen, simulieren die Täter durch Einsatz technischer Hilfsmittel eine Situation, die Nutzer dazu veranlasst, ihre Zugangsdaten preiszugeben. Initiiert wird ein solcher Angriff z. B. durch den Versand einer E-Mail-Nachricht an den Nutzer. In der E-Mail-Nachricht wird dem Nutzer ein Hyperlink mitgeteilt mit der Aufforderung, diesen zu öffnen. Klickt der Nutzer auf den Hyperlink, wird er in der Regel auf eine Internetseite geführt, die einen dem Benutzer bekannten, vermeintlich vertrauenswürdigen Webseitenbetreiber vortäuscht und die Möglichkeit zur Anmeldung mittels Eingabe von Zugangsdaten vorsieht. Der Nutzer wird dadurch veranlasst, seine vertraulichen Anmeldedaten preiszugeben. Ein Beispiel aus der Praxis ist der nachfolgende Fall: Im Berichtszeitraum erreichte mich eine Verletzungsmeldung gemäß Art. 33 DS-GVO eines Verantwortlichen mit Sitz in Hessen. Gegenstand der Meldung war, dass eine Beschäftigte durch einen Phishing-Angriff dazu bewegt worden war, ihre Zugangsdaten (Benutzername und Passwort) in einen vermeintlichen Web-Zugang zur betrieblich genutzten Microsoft Office 365-Plattform einzugeben. Mittels dieser Zugangsdaten konnten sich die Angreifer im Anschluss Zugriff auf das in der Microsoft Office 365-Plattform hinterlegte E-Mail-Konto der Beschäftigten verschaffen. Dieser Zugang wurde sodann genutzt, um hierüber weitere Phishing-Angriffe gegen den Verantwortlichen zu starten: Die Angreifer versandten Phishing-E-Mails über das E-Mail-Konto der Betroffenen an weitere Beschäftigte des Verantwortlichen.

Einige Mitarbeiterinnen und Mitarbeiter folgten dem in der Phishing-Nachricht enthaltenen Hyperlink und gaben in dem vorgeblichen Web-Zugang zur betrieblich genutzten Microsoft Office 365-Plattform ebenfalls ihre Zugangsdaten

ein. Dadurch wurde es den Angreifern ermöglicht, auf weitere betriebliche E-Mail-Konten zuzugreifen und hierüber erneut Phishing-Nachrichten zu versenden.

Obwohl der Verantwortliche bereits seit der ersten Phishing-Welle von der Vorgehensweise der Angreifer wusste, wiederholten sich die beschriebenen Phishing-Attacken mehrere Male. Die Angreifer konnten somit – unter Nutzung eines nahezu identischen Angriffsmusters und trotz Kenntnis des Verantwortlichen – innerhalb weniger Wochen mehrere gleichlaufende Phishing-Attacken erfolgreich durchführen.

Rechtliche Erwägungen

Gemäß Art. 5 Abs. 2 DS-GVO ist der Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DS-GVO enthaltenen Grundsätze rechenschaftspflichtig. Die Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO wird durch die Vorschrift des Art. 24 DS-GVO näher spezifiziert.

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").

Art. 24 DS-GVO

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. 2Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(…)

Art. 24 DS-GVO enthält mehrere unbestimmte Rechtsbegriffe, die auslegungsbedürftig sind. Unterstützen können hierbei die Art. 24 DS-GVO nachfolgenden Regelungen sowie die zugehörigen Erwägungsgründe der DS-GVO.

So ist für die Beurteilung der „geeigneten technischen und organisatorischen Maßnahmen" im Vorfeld zur Abwehr von Phishing-Attacken als auch zur Behebung nach Bekanntwerden z. B. Art. 32 Abs. 1 DS-GVO von Bedeutung.

Art. 32 DS-GVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(…)

Art. 32 Abs. 1 DS-GVO verdeutlicht, dass die zu ergreifenden technischen und organisatorischen Maßnahmen von dem mit der Datenverarbeitung verbundenen Risiko (risikobasierter Ansatz der DS-GVO) abhängig gemacht werden: Risikoreiche Verarbeitungen personenbezogener Daten erfordern striktere Maßnahmen, als dies bei risikoarmen Verarbeitungen der Fall ist.

Die objektive Beurteilung des Risikos ist daher zwingend, um feststellen zu können, wie die Rechte und Freiheiten natürlicher Personen wirksam zu schützen sind. Der Verantwortliche muss das Risiko somit evaluieren und abhängig vom ermittelten Risiko geeignete technische und organisatorische Maßnahmen ausgestalten.

Der Begriff des „Risikos für die Rechte und Freiheiten natürlicher Personen“ wird in den Erwägungsgründen 75, 76 und 94 Satz 2 der DS-GVO konkretisiert. Darüber hinaus kann das Kurzpapier Nummer 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Risikobeurteilung herangezogen werden (siehe auch 47. TB, Materialien Ziff. 4.7 oder abrufbar unter https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk). Das Papier erklärt zunächst den Begriff der Rechte und Freiheiten natürlicher Personen. Im Anschluss wird das Risiko – als das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann – definiert. Im Rahmen der Risikobeurteilung wird sodann empfohlen, die bestehenden Risiken zunächst zu identifizieren, eine Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden vorzunehmen und schließlich anhand der Begrifflichkeiten „geringes Risiko, Risiko und hohes Risiko“ zuzuordnen.

Nach der Evaluierung des mit der Verarbeitungstätigkeit verbundenen Risikos erfolgt die Zuweisung der geeigneten technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Umstände und der Zwecke der Verarbeitung,

mithin die Beurteilung der Frage des angemessenen Schutzniveaus. Hierzu führt Art. 32 Abs. 2 DS-GVO näher aus, dass insbesondere die Risiken zu berücksichtigen sind, die mit der Verarbeitung verbunden sind, d. h. insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Art. 32 Abs. 1 lit. a bis d DS-GVO sieht zur Gewährleistung des ermittelten Schutzniveaus verschiedene Maßnahmen vor, die jedoch nicht abschließend sind.

Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen (vgl. Art. 32 Abs. 1 lit. b DS-GVO), umfasst sowohl im Vorfeld zur Abwehr von Gefahren zu ergreifende als auch nach Bekanntwerden zur Behebung erforderliche technische und organisatorische Maßnahmen. Der Vorschrift kommt daher auch im Zusammenhang mit der Beurteilung von Phishing-Attacken besondere Bedeutung zu.

Aus Art. 32 Abs. 1 lit. d DS-GVO folgt, dass das Ergreifen technischer und organisatorischer Maßnahmen einer stetigen Fortentwicklung unterliegt. Der Regelung liegt u. a. der Gedanke zugrunde, dass sich Rahmenbedingungen von Verarbeitungstätigkeiten und somit Risiken und Angriffsszenarien mit der Zeit verändern und weiterentwickeln können. Auch die Verwendung des Begriffs „Stand der Technik“ macht deutlich, dass es sich lediglich um eine „momentane“ Bestimmung handelt, die regelmäßig evaluiert und weiterentwickelt werden muss.

Schließlich verdeutlicht Art. 32 Abs. 4 DS-GVO, dass der Verantwortliche auch innerhalb seiner eigenen Organisation alle notwendigen Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Hierzu gehört etwa, dass die im Hoheitsbereich des Verantwortlichen tätigen Personen auf die Einhaltung datenschutzrechtlicher Regelungen verpflichtet werden und in einem datenschutzgerechten Umgang mit personenbezogenen Daten geschult werden. Darüber hinaus sind Maßnahmen zu ergreifen, die einen Missbrauch personenbezogener Daten durch unterstellte Personen verhindern oder die Aufklärung entsprechender Vorfälle ermöglichen.

Festgestellte Versäumnisse

Vor dem Hintergrund dieser rechtlichen Erwägungen habe ich in technischer und organisatorischer Hinsicht bei meiner Prüfung bekannt gewordener Phishing-Attacken wiederholt folgende Versäumnisse seitens der Verantwortlichen festgestellt:

1. Im Vorfeld zu ergreifende Maßnahmen

– Unzureichende Absicherung des Authentifizierungs-Prozesses:

Vielfach mangelt es an angemessenen organisatorischen und technischen Maßnahmen zur Absicherung des Authentifizierungs-Prozesses. So fehlen beispielsweise verbindliche Passwortrichtlinien oder die geforderte Passwortkomplexität ist im Verhältnis zu den verarbeiteten personenbezogenen Daten inadäquat. Hinzu kommt, dass eine Authentifizierung mittels Benutzerkennung und Passwort in der Regel nur eine von mehreren Alternativen ist. Für die Microsoft Office 365-Plattform besteht bspw. auch die Möglichkeit zum Einsatz einer 2-Faktor-Authentifizierung (d. h. neben der Eingabe des Benutzernamens und des Passwortes wird ein weiterer „Faktor“ zur Authentifikation des Nutzers verwendet).

– Fehlende Regelungen zur Internet- und E-Mail-Nutzung am Arbeitsplatz:

Seitens der Verantwortlichen wurde häufig versäumt, eindeutige und verbindliche Regelungen zur Internet- und E-Mail-Nutzung am Arbeitsplatz zu treffen. So kann etwa eine geduldete, ungeregelte Privatnutzung des betrieblichen E-Mail-Kontos dazu führen, dass die Aufklärung von IT-Sicherheitsvorfällen – etwa durch Untersuchung eines kompromittierten E-Mail-Kontos – mit vermeidbaren Rechtsunsicherheiten einhergeht. Für die Evaluierung des Risikos für die Rechte und Freiheiten betroffener Personen ist es beispielsweise in der Regel erforderlich, eine Überprüfung von E-Mail-Inhalten und -Metadaten durchzuführen.

– Unzureichende technische und organisatorische Präventionsmaßnahmen:

Neben der Kernfunktionalität der E-Mail-Kommunikation bieten gängige E-Mail-Plattformen ergänzende Schnittstellen und Funktionalitäten. Hierzu zählen insbesondere auch solche aus dem Bereich der IT-Sicherheit, z. B. die Möglichkeit zur Integration von Virenscannern und eine Spam-Erkennung. Diese sollten entsprechend eingerichtet, genutzt und gewartet werden. Gleichzeitig sollten nicht benötigte Funktionalitäten und Dienste deaktiviert werden. Sie können Schwachstellen enthalten, die von Angreifern ausgenutzt werden könnten. Rein technische Lösungen sind in vielen Fällen jedoch nicht

ausreichend. So habe ich beispielsweise in einem Prüfverfahren festgestellt, dass selbst von der Plattform als potenzielle SPAM-E-Mails gekennzeichnete E-Mail-Nachrichten von Beschäftigten geöffnet wurden. Technische Maßnahmen müssen daher um organisatorische Maßnahmen ergänzt werden, um ihre volle Wirkung entfalten zu können. So sollten bspw. Vorgaben zum Umgang mit systemseitig als Spam identifizierten E-Mails definiert werden.

– Nicht vorhandene Notfallpläne:

Sollte es Dritten gelingen, durch Phishing ein oder mehrere E-Mail-Konten zu übernehmen, so kann der Faktor Zeit einen wesentlichen Einfluss auf die weitere Ausbreitung, die Tragweite und die Eindämmung von Phishing-Attacken haben. Dementsprechend sollten Verantwortliche über Notfallpläne verfügen, die ihnen eine schnelle, umfassende und wirksame Eindämmung der Phishing-Attacke ermöglichen. Dabei sollte nicht nur Wert auf die Erstellung entsprechender Dokumentationen gelegt werden, sondern die Praxistauglichkeit der Steuerung und Koordination sollte zusätzlich durch Notfallübungen überprüft werden.

– Fehlende Strukturen und Prozesse zur Behandlung von Verletzungsmeldungen:

Häufig ist festzustellen, dass es innerhalb der Organisationsstruktur des Verantwortlichen keine etablierten Prozesse zur Meldung und zum Umgang mit Verletzungen des Schutzes personenbezogener Daten gibt. So erkennen Beschäftigte häufig bereits nicht, dass sie durch ihr Verhalten Datenschutzrechte anderer Personen verletzt haben könnten. Auch ist den handelnden Personen häufig nicht bewusst, dass aufgrund der 72-Stunden-Frist des Art. 33 Abs. 1 Satz 1 DS-GVO umgehend nach Bekanntwerden der Verletzung des Schutzes personenbezogener Daten eine Meldung an die Aufsichtsbehörde zu erfolgen hat. Unklar ist oftmals auch, welche Personen seitens des Verantwortlichen zu informieren sind (z. B. Datenschutz- und IT-Sicherheitsbeauftragte). Es sollten daher vorab Prozesse etabliert werden, die eine strukturierte und effiziente Bearbeitung der Verletzung des Schutzes personenbezogener Daten ermöglichen.

– Mangelnde Effektivität der ergriffenen Schulungsmaßnahmen:

Zwar ist durchaus festzustellen, dass Verantwortliche bemüht sind, ihren Beschäftigten datenschutzrechtlich relevante Inhalte zu vermitteln. Auch können regelmäßig Verpflichtungen von Mitarbeitern zu Regelungen des Datenschutzes nachgewiesen werden (vgl. hierzu auch das Kurzpapier Nr. 19 der Konferenz des Datenschutzbeauftragten des Bundes und der Länder

zur „Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“ (abrufbar über https://datenschutz.hessen.de/infothek/kurzpapiere-der-dsk). Bei den meiner Behörde bekannt gewordenen Vorfällen zeigt sich aber, dass ein tatsächlich nachhaltiges Bewusstsein für datenschutzrechtliche Themen häufig nicht vorhanden ist. Dies zeigt sich etwa daran, dass – selbst wenn Strukturen und Prozesse zur Behandlung von Verletzungsmeldungen vorhanden sind – diese bei den Beschäftigten nicht ausreichend verinnerlicht sind und daher nicht zu einem effektiven Handeln im Sinne des Datenschutzes führen.

2. Nach Bekanntwerden ergriffene Maßnahmen

– Unterschätzung der Tragweite:

Häufig erfolgt im Rahmen von Phishing-Vorfällen eine starke Fokussierung auf die Überprüfung der E-Mail-Kommunikation. Gleichzeitig werden etwaige weiterreichende Auswirkungen nicht oder nur unzureichend betrachtet. Im Kontext von Microsoft Office 365-Plattform wird bspw. nicht berücksichtigt, dass das zur Authentifizierung am E-Mail-Postfach verwendete Benutzerkonto in der Regel auch für eine Authentifizierung an anderen Diensten der Plattform verwendet werden kann (z. B. Teams, Sharepoint, OneDrive). Es sollte daher darauf geachtet werden, dass von einzelnen Nutzerinnen und Nutzern nicht benötigte Dienste für deren Benutzerkonten gesperrt werden. Nur gesperrte Dienste müssen bei der Analyse von Phishing-Vorfällen nicht mitberücksichtigt werden. Je nach Ausgestaltung des Authentifizierungsprozesses sollte darüber hinaus geprüft werden, ob unter Umständen temporär sämtliche Benutzerkonten gesperrt werden müssen, um eine weitere Ausbreitung des Angriffs zu unterbinden. Vor einer Reaktivierung müssen in der Regel sämtliche Passwörter zurückgesetzt werden.

– Unzureichende Nachbereitung:

Neben den Notfallplänen sollten auch Maßnahmen ergriffen werden, die eine vollständige Analyse und Aufbereitung im Anschluss an eine Phishing-Attacke ermöglichen. Hierzu zählen z. B. eine datenschutzkonforme Protokollierung, anlassbezogene Schulungsmaßnahmen und die Überprüfung der Wirksamkeit der im Rahmen des Vorfalls ergriffenen Maßnahmen. Nur auf Basis einer angemessenen Nachbereitung und einer entsprechenden Dokumentation kann ein Verantwortlicher seinen Verpflichtungen aus der DS-GVO vollständig nachkommen.

– Unzureichende und verspätete Information betroffener Personen:

Betroffene Personen sind gemäß Art. 34 Abs. 1 DS-GVO über eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu informieren, falls diese voraussichtlich ein hohes Risiko für Rechte und Freiheiten der betroffenen Personen zur Folge hat und keine der Bedingungen aus Art. 34 Abs. 3 DS-GVO erfüllt ist. Dies setzt zunächst die Identifikation der betroffenen Person voraus. Anschließend muss für diese Personen das voraussichtliche Risiko für Rechte und Freiheiten sowie das Vorliegen der Bedingungen aus Art. 34 Abs. 3 DS-GVO ermittelt werden. Bei der Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen stelle ich fest, dass Verantwortliche sowohl die Anzahl der von einer Datenpanne betroffenen Personen als auch die potenziellen Risiken tendenziell unterschätzen. Auch fürchten viele Verantwortliche mögliche Image-Schäden, die mit der Erfüllung der Informationspflicht einhergehen können. Auch ist darauf zu achten, dass die Betroffenen transparent über geeignete Kommunikationsmittel und -wege über die Verletzung des Schutzes ihrer personenbezogenen Daten unterrichtet werden.

Rechtsfolgen festgestellter Versäumnisse im Rahmen einer Meldung gemäß Art. 33 DS-GVO

Grundsätzlich ist zu beachten, dass Versäumnisse, die im Rahmen einer Prüfung nach Art. 33 DS-GVO festgestellt werden, weitergehende aufsichtsbehördliche Verwaltungs- und Bußgeldverfahren nach sich ziehen können.

4.4
Verwendung alter Bewerbungsunterlagen

Daten aus einem abgeschlossenen Bewerbungsverfahren dürfen ohne Einwilligung der betroffenen Bewerber nicht für ein erneutes Auswahlverfahren genutzt werden. Dies gilt auch für die Bewerbung auf den Posten eines 1. Stadtrats in einer Kommune.

In einer hessischen Kommune war die Stelle des ersten Stadtrats ausgeschrieben. Der Wahlvorbereitungsausschuss der Kommune konnte sich nicht auf einen Kandidaten unter den Bewerbern einigen. Man beschloss daraufhin, die Stelle erneut auszuschreiben und ein privates Unternehmen mit der Abwicklung des Bewerbungsverfahrens zu betrauen. Dieses Unternehmen erbat für das zweite Auswahlverfahren die Bewerbungsunterlagen der Bewerber aus dem ersten Verfahren und erhielt diese auch.

Dieser Sachverhalt wurde mir von einem Mitglied der Stadtverordnetenversammlung vorgetragen, der in diesem Vorgehen einen Verstoß gegen datenschutzrechtliche Bestimmungen vermutete.

Bewerberdaten sind Beschäftigtendaten gem. § 23 Abs. 8 Satz 2 HDSIG und dürfen für die Dauer des Auswahlverfahrens von der einstellenden Stelle verarbeitet werden. Nach Abschluss des Auswahlverfahrens sind die Daten der nicht berücksichtigten Bewerber an diese zurückzugeben oder zu vernichten. Etwas anderes kann nur dann gelten, wenn die Bewerber ausdrücklich in die Verwendung für ein weiteres Bewerbungsverfahren eingewilligt haben. In dem vorgetragenen Fall lag eine Einwilligung der Bewerber aus dem ersten Bewerbungsverfahren eindeutig nicht vor.

§ 23 Abs. 8 Satz 2 HDSIG

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

Diese Grundsätze gelten auch für die Besetzung der Position des 1. Stadtrats oder 1. Beigeordneten, auch wenn die Auswahlentscheidungen durch ein anderes Gremium getroffen werden.

Die fragliche Kommune, die die Bewerberdaten für das zweite Auswahlverfahren an das private Unternehmen weitergeben hatte, bekam offensichtlich ebenfalls Zweifel an der Rechtmäßigkeit dieser Datenverwendung; denn sie meldete kurz nach Anzeige durch den Stadtverordneten die Weitergabe als Fall nach Art. 33 DS-GVO (Datenpanne) bei meiner Behörde.

Ich habe die Kommune aufgefordert, die beauftragte Firma anzuweisen, die übersandten Daten unverzüglich zu löschen und eine Löschbescheinigung anzufordern und mir diese zu übersenden. Dies ist geschehen.

5. Allgemeine Verwaltung, Kommunen

5.1
Übermittlung von Jubiläumsdaten nach dem Bundesmeldegesetz

Kommunale Mitteilungsblätter sind nicht vom Pressebegriff umfasst, daher kann § 50 Abs. 2 Bundesmeldegesetz hier nicht zur Anwendung kommen.

Datenübermittlungen von Jubiläumsdaten an die Presse nach § 50 Abs. 2 Bundesmeldegesetz (BMG) sind immer wieder Gegenstand von Anfragen und Beschwerden.

§ 50 BMG

(2) Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über

1. *Familienname,*
2. *Vornamen,*
3. *Doktorgrad,*
4. *Anschrift sowie*
5. *Datum und Art des Jubiläums.*

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

Die Regelung stellt dabei klar und deutlich die Voraussetzungen, den Rahmen und die Adressaten der Datenübermittlungen dar, unter denen die Meldebehörde Daten übermitteln darf. Aus der Formulierung ergibt sich, dass es sich nicht um ein Gebot handelt, d. h., es besteht seitens der Adressaten keinesfalls ein Rechtsanspruch auf die Datenübermittlung. Diese kann durch die Kommune auch abgelehnt oder in ihrem Umfang reduziert werden. Beispielsweise kann darauf verzichtet werden, dass auch die Anschrift der Jubilare übermittelt wird.

Zu Fehlbeurteilungen kommt es jedoch im Zusammenhang mit dem Pressebegriff. Dieser ist grundsätzlich recht weit gefasst, so dass etwa auch Kirchenzeitungen und Anzeigenblätter hier Adressat der Daten aus dem Melderegister sein dürfen. Kommunale Mitteilungsblätter werden vom Pressebegriff jedoch nicht mit umfasst. Es dürfen daher auch innerhalb einer Kommune keine Daten zum Zwecke der Veröffentlichung i. S. d. § 50 Abs. 2 BMG übermittelt bzw. weitergegeben werden.

Die Widerspruchsmöglichkeiten gem. § 50 Abs. 5 BMG sowie das diesbezügliche Hinweisungsgebot erscheinen mir vor dem Hintergrund der aktuellen datenschutzrechtlichen Regelungen der DS-GVO nicht mehr zeitgemäß.

§ 50 BMG

(5) Die betroffene Person hat das Recht, der Übermittlung ihrer Daten nach den Absätzen 1 bis 3 zu widersprechen; hierauf ist sie bei der Anmeldung nach § 17 Absatz 1 sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen.

Eine aktive Einwilligung zur Datenübermittlung wäre der bisherigen Regelung eines aktiven Widerspruchs gegenüber zu bevorzugen.

5.2
Unterstützungsunterschrift für einen Wahlvorschlag

Zum Nachweis, dass ein Wähler einen Wahlvorschlag unterstützt hat, darf nur dies bei der Gemeinde dokumentiert werden und nicht, welchen Wahlvorschlag er unterstützt hat.

Ein Bürger wandte sich an meine Behörde und schilderte mir folgenden Sachverhalt: Er habe für die anstehende Europawahl einen Wahlvorschlag in seiner Heimatgemeinde unterstützt und sich deshalb zum Bürgerbüro begeben, um sich sein Wahlrecht bescheinigen zu lassen. Im Bürgerbüro habe die Mitarbeiterin dann zu Dokumentationszwecken das gesamte Formblatt für eine Unterstützungsunterschrift kopiert und zu den Akten genommen. Daraus ergab sich auch, welchen Wahlvorschlag der Bürger mit seiner Unterschrift unterstützt hatte.

Die Wahlordnungen geben eindeutige Vorgaben, was im Falle der Wahlrechtsbescheinigung von Unterstützungsunterschriften zu dokumentieren ist.

§ 32 Abs. 5 Satz 2 EuWO

(5) ²Die Gemeindebehörde darf für jeden Wahlberechtigten die Bescheinigung des Wahlrechts nur einmal erteilen; dabei darf sie nicht festhalten, für welchen Wahlvorschlag die erteilte Bescheinigung bestimmt ist.

Für die Unterstützungsunterschriften zur Europawahl wird das Formblatt Anlage 14 zur Europawahlordnung verwendet. Dies weist in einer Fußnote noch einmal eindeutig darauf hin, dass nicht festgehalten werden darf, welcher Wahlvorschlag mit der Unterschrift unterstützt wird.

Die Kommune hatte mit der Kopie des gesamten Formblattes eindeutig gegen die Vorschrift der Europawahlordnung verstoßen. Ich habe deshalb verlangt, dass sie den Teil, der die zu unterstützende Partei anbelangt, aus ihren Unterlagen entfernt. Dies wurde mir bestätigt.

Da der Petent sich auch an den Bundeswahlleiter gewandt hatte, wurde auch von diesem die Entfernung der Information über die unterstützte Partei verlangt, wie mir die Gemeinde mitteilte.

5.3
Erteilung von Auskünften zu Grundstückseigentümern durch die Gemeinden

Anfragende, die bei Kommunen Informationen über Eigentümer der dort belegenen Grundstücke wünschen, müssen an das Landesamt/ Ämter für Bodenmanagement verwiesen werden.

In der Beratungs- und Beschwerdepraxis der letzten Jahre taucht wiederholt die Frage auf, ob eine Kommune einem Dritten Auskünfte zu den Eigentümern eines in der Gemeinde belegenen Grundstücks erteilen darf. Bauträger, Infrastrukturentwicklungsverbände, private Initiativen oder auch Nachbarn wenden sich an die Gemeinden der dort belegenen Grundstücke und wollen Auskunft über die Grundstückseigentümer haben. Zur Absicherung der Datenübermittlung stellen die Gemeinden bei mir Anfragen über die datenschutzrechtliche Zulässigkeit dieser Auskünfte.

Sämtliche grundstücksbezogenen Informationen in Hessen werden in Liegenschaftskatastern geführt. Diese bei der Landesverwaltung für Bodenmanagement geführten Kataster sind öffentliche Register, die jeder Person zur Einsicht und Auskunft offenstehen. Die Einsicht in die Namen, die Geburtsdaten und die Anschriften der Eigentümer steht allerdings nach § 16 Abs. 2 des Hessischen Gesetzes über das öffentliche Vermessungs- und Geoinformationswesen (HVGG) nur den Personen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben.

§ 16 Abs. 1 und 2 HVGG

(1) Jede Person oder Stelle kann die Datenbanken des öffentlichen Vermessungswesens als allgemein zugängliche Quellen einsehen sowie Auskünfte oder Ausgaben daraus erhalten.

(2) Abweichend von Abs. 1 stehen die Einsicht in die Namen, die Geburtsdaten und die Anschriften der Eigentümerinnen und Eigentümer sowie entsprechende Auskünfte und Ausgaben nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Entsprechendes gilt für die Daten der Bevollmächtigten. Das berechtigte

Interesse ist darzulegen. Die Empfänger dürfen diese Daten nur für den Zweck nutzen, der das berechtigte Interesse begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden. Satz 3 gilt nicht für

1. *dinglich Berechtigte,*
2. *Behörden des Landes und kommunale Gebietskörperschaften in Erfüllung ihrer Aufgaben,*
3. *öffentlich bestellte Vermessungsingenieurinnen und Vermessungsingenieure sowie Notarinnen und Notare, soweit die personenbezogenen Daten im Einzelfall zur Erfüllung ihrer Aufgaben benötigt werden.*

Die Kommunen haben in der Regel im Rahmen der Teilnahme an einem automatisierten Abrufverfahren die Möglichkeit, auf die Daten aus dem Liegenschaftskataster zuzugreifen. Diese Zugriffsberechtigung besteht aber nur für die Fälle, in denen die Daten zur Erfüllung der kommunalen Aufgaben erforderlich sind (§ 16 Abs. 2 Satz 5 Nr. 2 HVGG). Dies wird auch in den entsprechenden Nutzungsverträgen zwischen der Landesverwaltung für Bodenmanagement und den Kommunen festgehalten.

Die Beantwortung von Anfragen von Dritten, die die Daten zu den Grundstückseigentümern für ihre eigenen Zwecke benötigen, findet gerade nicht im Rahmen der Erfüllung von kommunalen Aufgaben statt. Nutzen die Kommunen ihre Zugangsberechtigung für die Erteilung der entsprechenden Auskünfte an Dritte, übermitteln sie personenbezogene Daten ohne eine datenschutzrechtliche Grundlage. Auf Art. 6 Abs.1 Satz 1 lit. c DS-GVO in Verbindung mit § 16 Abs. 2 Satz 1 HVGG können sie diese Datenübermittlung nicht stützen, weil von der Verpflichtung zur Auskunftserteilung nach § 16 Abs. 2 Satz 1 HVGG nur die auskunftsverpflichtete Landesverwaltung für Bodenmanagement betroffen ist.

Als für die Anfragen Dritter über die Grundstückseigentümer originär zuständige Stelle ist die Landesverwaltung für Bodenmanagement berechtigt, für die Erteilung der Auskünfte Gebühren zu verlangen, um den Aufwand, der ihr für die Unterhaltung des Liegenschaftskatasters entsteht, zu kompensieren. Im Falle der Erteilung der Auskünfte durch die Gemeinde entgehen der Landesverwaltung für Bodenmanagement unberechtigterweise diese Gebühren. Außerdem ist zu beachten, dass die nötige Kompetenz und Erfahrung bei der Feststellung des berechtigten Interesses im Sinne von § 16 Abs. 2 Satz 1 HVGG nur bei der Landesverwaltung für Bodenmanagement vorhanden ist.

Die Kommunen müssen daher die Anfragenden auf die Landesverwaltung für Bodenmanagement verweisen. Die Auskunftsberechtigten dürfen die so erhaltenen Daten der Grundstückseigentümer nur zweckgebunden nutzen (§ 16 Abs. 2 S. 4 HVGG).

5.4
Ausgestaltung von Bürgerbefragungen durch öffentliche Stellen

Im vergangenen Jahr hat der HBDI immer wieder öffentliche Stellen bei der Ausgestaltung und Umsetzung von Befragungen beraten. Hierbei handelte es sich um diverse Themen, die von einer einfachen Bürgerbefragung zum Sicherheitsgefühl in der eigenen Region, einer Hebammenbefragung bis hin zu einer Abfrage zur Gewalterfahrung in der öffentlichen Verwaltung gingen. Im Folgenden soll über die wesentlichen Beratungsinhalte informiert werden.

Bezeichnungen der Befragungen als anonym – Hebammenbefragung

Bei einer Vielzahl von Befragungen wurde seitens der erhebenden Stelle davon gesprochen, dass die Befragung „vollkommen anonym" sei. Hierbei wurde leider häufig außer Acht gelassen, dass gerade das Zusammenspiel der erhobenen Daten sehr wohl zu einer Personenbeziehbarkeit führt. Beispielhaft zu erwähnen ist hier eine geplante Befragung von Hebammen. Anhand des vorliegenden Fragebogens konnte nicht mehr von einer „anonymen Befragung" ausgegangen werden. So war es mir bereits anhand von vier Fragen möglich, eine konkrete Person zu identifizieren. Die genannten Fragen lauteten wie folgt:

– Sind Sie Mitglied in einem Berufsverband oder bei einer Fachgesellschaft? (Antwort: Nein oder Ja und zwar namentlich zu nennender Verband)
– In welchem Landkreis bzw. in welcher kreisfreien Stadt sind Sie hauptsächlich tätig?
– In welchem Jahr sind Sie geboren?
– Welche Leistungen, die nicht nach § 134a SGB V vergütet werden, bieten Sie an?

Die Fragen wurden anhand eines Beispiels durchgeprüft und beispielhaft beantwortet. Die Auswahl traf ein Mitglied im Bund freiberuflicher Hebammen Deutschlands e. V. (BfHD), das im Schwalm-Eder-Kreis tätig ist und beispielhaft das Geburtsjahr 1960 hat. Auf der Homepage des Verbandes gab es letztlich nur noch eine Person, die auch als Zusatzleistung die Akupunktur anbietet. Damit stand im Ergebnis fest, dass nur eine Person den Fragebogen entsprechend ausgefüllt haben konnte.

Weitere Beispiele dieser Art waren denkbar, so dass in den gesamten Dokumenten der Begriff der Anonymität herauszustreichen gewesen wäre. Ebenso war von der Zusicherung abzurücken, dass keine Rückschlüsse auf einzelne Personen möglich sind. Das Gleiche galt für die Zusicherung, dass die Datenerhebung und die eingesetzten Messinstrumente nicht geeignet sind, einzelne Personen – auch nicht über die Angabe von Merkmalen oder

Merkmalskombinationen – identifizieren zu können. Vielmehr sollte nach Auffassung meines Hauses darüber aufgeklärt werden, dass die erhobenen Daten unter Umständen personenbeziehbar sein können, dass jedoch mittels technisch/organisatorischer Maßnahmen der Personenbezug entfernt wird und nicht versucht wird, eine Reidentifizierung zu erreichen. Das entsprechende Risiko ist mithin klar und transparent zu benennen.

Zudem ist grundsätzlich bei derartigen Befragungen zu überlegen, ob einzelne Fragen mit einem hohen Reidentifizierungsfaktor gestrichen werden können oder ob diese tatsächlich für die spätere Auswertung erforderlich sind. Die Erforderlichkeit ist entsprechend zu begründen.

Alternativ sollte auch immer die Möglichkeit bedacht werde, größere Kategorien zu bilden, in die sich der teilnehmende Befragte eintragen kann. So sind etwa Geburtsjahrgänge zu bilden und grob gerasterte Zeiträume anzugeben anstatt eines exakten Jahres. Dies mindert die Gefahr, mit weiteren Angaben zu einer Reidentifizierung der teilnehmenden Person zu gelangen.

Im Ergebnis wurde von der verantwortlichen Stelle der Wunsch geäußert, weiterhin an einer Bezeichnung der Befragung als anonym festzuhalten. Hierzu wurde nicht mehr der konkrete Berufsverband oder die Fachgesellschaft abgefragt. Auch die Frage zum Erhalt des Hebammenexamens wurde grob gerastert. Ebenso wurde das Alter nunmehr nur noch in Kategorien abgefragt. Gestrichen wurde auch die Frage zum Geschlecht. Gerade bei Hebammen war insofern davon auszugehen, dass es nur eine ganz geringe Zahl an männlichen Hebammen gibt.

Auch die Frage nach der durchschnittlichen Entfernung des Arbeitsplatzes vom Wohnort entfiel. Im Falle einer anderen Studie betreffend das Sicherheitsgefühl in der Bevölkerung wurde zudem darauf hingewiesen, dass es sich anbietet, nur Ortsteile einzubeziehen, die auch eine gewisse Einwohnerzahl erreichen. Auf diese Weise kann das Risiko der Reidentifizierung ebenfalls minimiert werden.

Sonderkonstellation bei der Umfrage zur Gewalt gegen Beschäftigte im öffentlichen Dienst im Land Hessen

Eine besondere Konstellation hatte ich letztlich bei einer Befragung, welche die Gewalterfahrung von öffentlich Bediensteten zum Gegenstand hatte. Bei der ursprünglichen Ausgestaltung der Befragung war es zwingend vorgesehen, dass der Befragte auch namentlich die Behörde benennt, in der er tätig ist. Dies stellte insbesondere bei kleineren Behörden, wie beispielsweise bei meiner eigenen Dienststelle, ein Risiko der Reidentifizierung dar. Sofern hier außerdem eine Kombination aus beruflicher Funktion (z. B. Referatsleiter)

und Beruf (z. B. Volljurist) abgefragt wird, ist nahezu von einer 100 %-igen Identifizierbarkeit auszugehen. Ich habe daher noch einmal versucht, mit der verantwortlichen Stelle abzuklären, ob die Angabe der konkreten Behörde tatsächlich erforderlich ist.

Auch der Zusatz, dass die eigene Behörde nur bei einem gewissen Mitarbeiterumfang zu benennen ist, konnte meines Erachtens das verbleibende Restrisiko nicht komplett ausschließen. Gerade der Begriff „sehr kleine Behörde" ist hierfür zu unbestimmt. Für die Teilnehmer ist letztlich nicht ersichtlich, ab wann man von sehr kleinen Einheiten spricht, bzw. ob ihre eigene Stelle davon betroffen ist. Zudem wird eine Reidentifikation auch bei Behörden mit mehr als 100 Mitarbeitern möglich sein, sofern diese namentlich benannt werden.

Die verantwortliche Stelle teilte mir daraufhin noch einmal mit, dass es für die Auswertungen fundamental wichtig sei, dass man die Branchen bzw. Dienststellen „beruflich" einordnen könne. Damit war aber meines Erachtens die Angabe der Dienststelle nicht entscheidend, sondern das Berufsfeld. Die Abfrage sollte daher generell lauten: „Bitte geben sie das Berufsfeld (grob) an, in dem sie arbeiten." Eine entsprechende Änderung wurde letztlich vorgenommen, so dass nicht mehr der konkrete Arbeitgeber, sondern lediglich das Berufsfeld abgefragt wurde (Bildung, Gesundheit und Pflege, Justiz, Verwaltung oder Sonstiges).

Beratung im Kontext von Online-Befragungen

Häufig erhalte ich auch Beratungsanfragen zu Umfragen, bei denen die Daten Online erhoben werden sollen. Hierzu erreichte mich auch die Frage, ob man entsprechende Online-Befragungen mit dem Programm Survey Monkey durchführen könne und ob dieses Programm per se als Mittel betrachtet werden kann, das zur Durchführung von anonymen Umfragen verwendet werden kann.

Hierzu teilte ich mit, dass Survey Monkey ein weit verbreitetes Werkzeug für entsprechende Umfragen ist. Umfragen mit Survey Monkey sind jedoch nicht automatisch anonym. Hier müssen mindestens spezielle Einstellungen vorgenommen werden (siehe auch How-do-I-make-surveys-anonymous unter help.surveymonkey.com). Hinzu kommen Server-logs (siehe Datenschutzerklärung). Die Aussage, dass Survey Monkey verwendet wird und dass keine personenbezogenen Daten abgefragt werden, reicht nicht aus. Hier sind zusätzliche Maßnahmen erforderlich.

Bei der entsprechenden Online-Befragung bin ich im Übrigen auch darauf gestoßen, dass der Fragebogen zwar als anonym beworben wurde, der Teilnehmende aber gleichzeitig auf der letzten Seite darüber aufgeklärt wird,

dass der Fragebogen versandt werden kann. Hier wird unter anderem eine E-Mail-Adresse angegeben. In diesem Kontext fehlte der Hinweis, dass der Versand der E-Mail dazu führt, dass die Abgabe nicht mehr anonym ist. Gleiches gilt für den Fall, dass ein postalischer Versand mit Angabe des Absenders erfolgt.

Im Ergebnis habe ich für künftige Befragungen auch hier den Verzicht auf die nicht korrekte Bezeichnung als anonym empfohlen, da der Teilnehmer ansonsten falsch und nicht informiert aufgeklärt wird. Es sollte vielmehr davon gesprochen werden, dass die Antworten bei Eingang personenbeziehbar sind, aber mittels technischer und organisatorischer Maßnahmen der Personenbezug entfernt und auf eine Anonymisierung hingewirkt wird.

Abschließende Anmerkung

Auch künftig wird meine Dienststelle gerne beratend bei entsprechenden Befragungen tätig werden. Hilfestellung kann insoweit insbesondere immer dann gegeben werden, wenn es um Fragen der ausreichenden Anonymisierung, Transparenz und Informiertheit der Einwilligung geht. Dies betrifft insbesondere auch die bei entsprechenden Umfragen verpflichtend vorzusehende Information nach Art. 13 DS-GVO.

6. Polizei, Justiz, Soziales

6.1
Kontrolle meiner schriftlichen Kommunikation mit Strafgefangenen

Die schriftliche Kommunikation meiner Behörde mit Strafgefangenen unterliegt nicht der Postkontrolle in hessischen Justizvollzugsanstalten.

Mich erreichten schriftliche Mtiteilungen Gefangener hessischer Justizvollzugsanstalten, die unter anderem Beschwerde darüber führten, dass auch die von mir an sie gerichtete Post sie nur geöffnet erreichte. Die zugrundeliegenden rechtlichen Regelungen in § 33 Abs. 4 Hessisches Strafvollzugsgesetz besagen, dass die Kommunikation zwischen Strafgefangenen und den in § 119 Abs. 4 Satz 2 Strafprozessordnung (StPO) genannten Stellen nicht überwacht wird. In § 119 Abs. 4 Satz 2 Nr. 7 StPO sind die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständigen Stellen der Länder explizit genannt.

§ 33 HessStVollzG

(4) Nicht überwacht werden auch Kontakte mit den in § 119 Abs. 4 Satz 2 der Strafprozessordnung genannten Personen und Stellen, soweit

1. *bei mündlicher Kommunikation die Identität der Kontaktperson zweifelsfrei feststeht,*
2. *ausgehende Schreiben an den jeweiligen Dienstsitz gerichtet sind und den Absender zutreffend angeben oder*
3. *bei eingehenden Schreiben begründete Zweifel an der Identität des Absenders nicht vorliegen oder auf andere Weise als durch Überwachung ausgeräumt werden können.*

§ 119 StPO

(4) Die §§ 148, 148a bleiben unberührt. Sie gelten entsprechend für den Verkehr des Beschuldigten mit

7. *dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, den für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständigen Stellen der Länder und den Aufsichtsbehörden nach § 40 des Bundesdatenschutzgesetzes,*

(…)

Sofern also keine Zweifel daran bestehen, dass ich der Absender oder auch Adressat von Kommunikation mit Strafgefangenen bin, darf hier keine Kontrolle der schriftlichen Kommunikation erfolgen.

Um eine diesbezügliche Einschätzung seitens der JVA-Bediensteten zu erleichtern, werde ich das „Brief in Brief“-Verfahren nutzen, d. h. das kuvertierte

Schreiben an die Strafgefangenen oder den Strafgefangenen befindet sich in einem an die betreffende JVA gerichteten Umschlag mit Anschreiben, in dem nochmals auf den Absender und eine telefonische Möglichkeit der Kontaktaufnahme zu Überprüfungszwecken hingewiesen wird.

6.2
Löschung von unvollständigen Datensätzen in POLAS-Hessen

Soweit personenbezogene Datensätze zu Straftaten im polizeilichen Informationssystem POLAS-Hessen gespeichert sind, muss dort auch eine Information über den Verfahrensausgang hinterlegt sein.

Die Hessische Polizei betreibt auf rechtlicher Grundlage des § 20 Abs. 6 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) ein polizeiliches Informationssystem. Mit diesem System werden Daten, die im Zusammenhang mit der Verfolgung von Straftaten gewonnen wurden, für Zwecke der vorbeugenden Kriminalitätsbekämpfung genutzt.

§ 20 Abs. 6 HSOG

(6) [1]Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere Rechtsvorschriften nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten weiterverarbeiten. Soweit es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben, sind die Daten zu löschen, sobald der Verdacht entfällt.

Konkret handelt es sich um den Datenbestand, der regelmäßig beispielsweise bei Personenkontrollen, aber auch bei Zuverlässigkeitsüberprüfungen abgefragt wird. Sofern dort personenbezogene Daten zu Straftaten hinterlegt sind, betreffen diese immer tatverdächtige, beschuldigte oder verurteilte Personen. Sofern dort Daten über Personen vorhanden sind, ist dieser Datenbestand für die betreffende Person grundsätzlich nachteilig, insbesondere im Zusammenhang mit Zuverlässigkeitsüberprüfungen. Diese sind in verschiedenen Bereichen gesetzlich geboten, beispielsweise im Zusammenhang mit waffenrechtlichen Erlaubnissen, bei Tätigkeitsaufnahmen in sensiblen Bereichen öffentlicher Stellen oder auch bei privilegiertem Zugang zu besonders gefährdeten Veranstaltungen.

Eine Besonderheit dieses Datenbestandes ist, dass die Daten, die erfolgte Straftaten betreffen, zu einem Zeitpunkt erfasst und der Polizei zum Abruf zur Verfügung gestellt werden, an dem weder von der zuständigen Staatsanwaltschaft noch von einem Gericht abschließend über das Strafverfahren

entschieden wurde. Erst nach einer solchen Entscheidung einer Staatsanwaltschaft oder eines Gerichts wird der Verfahrensausgang gemäß § 482 StPO an die Polizei übermittelt und in POLAS-Hessen hinterlegt, soweit sie nicht unmittelbar zu einer Löschung des betreffenden Datensatzes führt.

§ 482 StPO

(1) Die Staatsanwaltschaft teilt der Polizeibehörde, die mit der Angelegenheit befasst war, ihr Aktenzeichen mit.

(2) [1]Sie unterrichtet die Polizeibehörde in den Fällen des Absatzes 1 über den Ausgang des Verfahrens durch Mitteilung der Entscheidungsformel, der entscheidenden Stelle sowie des Datums und der Art der Entscheidung. Die Übersendung der Mitteilung zum Bundeszentralregister ist zulässig, im Falle des Erforderns auch des Urteils oder einer mit Gründen versehenen Einstellungsentscheidung.

(3) In Verfahren gegen Unbekannt sowie bei Verkehrsstrafsachen, soweit sie nicht unter die §§ 142, 315 bis § 315c des Strafgesetzbuches fallen, wird der Ausgang des Verfahrens nach Absatz 2 von Amts wegen nicht mitgeteilt.

(4) Wird ein Urteil übersandt, das angefochten worden ist, so ist anzugeben, wer Rechtsmittel eingelegt hat.

Daher haben diese Datensätze, solange dort keine Mitteilung über den Verfahrensausgang hinterlegt ist, eine noch mit Vorbehalten behaftete Aussagekraft. Dieser Zeitraum zwischen polizeilicher Erfassung der Daten und einer Mitteilung über den Verfahrensausgang ist daher datenschutzrechtlich nicht unproblematisch.

Nach erfolgter Mitteilung von Verfahrensausgängen der Staatsanwaltschaften an die Polizei kann sich eine weitere Problematik ergeben. Staatsanwaltschaftliche Verfahrenseinstellungen auf Grundlage des § 170 Abs. 2 StPO Strafprozessordnung bedeuten, dass die Ermittlungen nicht genügend Anlass zur Erhebung der öffentlichen Klage bieten.

§ 170 StPO

(1) Bieten die Ermittlungen genügenden Anlaß zur Erhebung der öffentlichen Klage, so erhebt die Staatsanwaltschaft sie durch Einreichung einer Anklageschrift bei dem zuständigen Gericht.

(2) [1]Andernfalls stellt die Staatsanwaltschaft das Verfahren ein. Hiervon setzt sie den Beschuldigten in Kenntnis, wenn er als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen war; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse an der Bekanntgabe ersichtlich ist.

Dies kann durch die staatsanwaltschaftliche Feststellung, dass der Tatverdacht ausgeräumt ist oder die Straftat nicht stattgefunden hat, ausgelöst werden und

führt dann grundsätzlich zu einer Löschung des betreffenden polizeilichen Datenbestandes in POLAS-Hessen zu dieser Straftat. Soweit eine Einstellung gem. § 170 Abs. 2 StPO aufgrund mangelnden Tatverdachtes erfolgt, trifft die Polizei eine eigene fachliche Entscheidung zum Erfordernis der weiteren Speicherung in POLAS-Hessen, in die regelmäßig eine aussagekräftige Einstellungsbegründung der Staatsanwaltschaft einbezogen werden muss.

Meine Überprüfungen aufgrund von Beschwerden in Einzelfällen ergaben, dass bei einzelnen Datensätzen in POLAS-Hessen zu Straftaten auch Jahre nach der Tatbegehung keine Daten zu Verfahrensausgängen hinterlegt waren. Bei von mir beim Hessischen Landeskriminalamt (HLKA) initiierten Überprüfungen ist vereinzelt festgestellt worden, dass auch bei den zuständigen Staatsanwaltschaften keine Informationen über die betreffenden Verfahrensausgänge mehr erlangt werden konnten. In diesen Fällen kann demnach auch nicht ausgeschlossen werden, dass man seitens der zuständigen Staatsanwaltschaft den Tatverdacht als ausgeräumt ansah oder feststellte, dass die Tat nicht stattgefunden hat bzw. es keine Straftat war. Ein solcher Datensatz ist daher nach meiner Einschätzung zu löschen.

Die Polizei hat bezüglich der Datenspeicherungen in POLAS-Hessen in § 20 Abs. 6 HSOG eine eigene und unabhängige Rechtsgrundlage und darf in deren Rahmen in eigener Fachlichkeit über das Erfordernis der Daten zum Zwecke der präventiven Kriminalitätsbekämpfung befinden. Da abschließende Mitteilungen von Staatsanwaltschaften und Gerichten zu Verfahrensausgängen jedoch zu Löschungen der Datenbestände führen können, sind diese aus datenschutzrechtlichen Gründen immer durch die Polizei zu bewerten und müssen daher auch immer vorliegen.

6.3
Zum Umgang mit (anonymen) Hinweisgebern an die Sozialverwaltung

Der Umgang mit Hinweisen aus der Bevölkerung an die Sozialverwaltung eröffnet ein Spannungsfeld, das für den behördlichen Hinweisnehmer nicht immer einfach zu behandeln ist. Es gilt auch in diesen Fallkonstellationen der datenschutzrechtliche Grundsatz der Direkterhebung bei Betroffenen sowie der Vorrang der Vorgaben des Sozialdatenschutzes vor denen des Sozialverwaltungsverfahrens.

Mich erreichte die Beschwerde eines SGB-Leistungsempfängers, der in Folge einer Frühverrentung seit einigen Jahren sowohl Leistungen aus der gesetzlichen Rentenversicherung als auch ergänzend Leistungen zur Grundsicherung gemäß SGB XII durch das Sozialamt bezog. Anfang Mai

2019 erhielt er ein Schreiben des Sozialamtes, in dem die Einstellung der Leistungen gemäß SGB XII zum nächsten Monatsersten angekündigt wurde. Gleichzeitig wurde er aufgefordert, Nachweise für einen möglichen Weiterbezug der Sozialleistungen vorzulegen. Zur Begründung wurde erklärt, dass Informationen vorlägen, wonach ein weiterer Anspruch auf Leistungen ausscheiden würde. Dem Betroffenen wurde in diesem Schreiben ein Sachverhalt dargestellt, den das Sozialamt offenbar als Hinweis erhalten hatte und als Tatsache anerkannte. Die Versuche des Betroffenen, vom Sozialamt zu erfahren, wer die Informationen mitgeteilt habe, scheiterten. Das Sozialamt berief sich gegenüber dem Betroffenen auf Informantenschutz und ein höheres schutzwürdiges Interesse des Hinweisgebers gegenüber den Interessen des Betroffenen auf eine Auskunftserteilung. Hierüber beschwerte sich der Betroffene bei mir und bat mich um eine datenschutzrechtliche Einschätzung bzw. Intervention beim Sozialamt.

Sachverhaltsaufklärung

Auf meine Aufforderung hin nahm das Sozialamt zunächst zum Fall Stellung. Danach bezog der Betroffene Leistungen nach dem Dritten Kapitel des SGB XII, als durch ein anonymes Schreiben am 22. April 2019 der Hinweis bei der Behörde einging, wonach der Betroffene am selben Tag zu einem mehrmonatigen Auslandsaufenthalt aufgebrochen sei. Da eine Gewährung von Leistungen ab einem Auslandsaufenthalt von mehr als 28 Tagen nach § 41a SGB XII nicht zulässig sei, habe man ihm daraufhin per Bescheid vom 02.05.2019 mitgeteilt, dass die Leistung ab dem 01.06.2019 bis zum Nachweis seiner Rückkehr eingestellt würde.

§ 41a SGB XII

Leistungsberechtigte, die sich länger als vier Wochen ununterbrochen im Ausland aufhalten, erhalten nach Ablauf der vierten Woche bis zu ihrer nachgewiesenen Rückkehr ins Inland keine Leistungen.

Da die Verfasserin bzw. der Verfasser des Schreibens ausdrücklich um Anonymität bat, wurde dem Betroffenen auf seine Nachfrage diese Auskunft verweigert. Der anonyme Hinweis sei vom Sozialamt zur Kenntnis genommen und, im Rahmen der Ermessensentscheidung, Anlass für das Schreiben an den Betroffenen gewesen. Die hinweisgebende Person habe keine Informationen über die Reaktion der Behörde erhalten.

Da die Sozialverwaltung zur Erfüllung ihrer gesetzlichen Aufgaben auf derartige Unterstützung aus der Bevölkerung angewiesen sei, würden Eingaben grundsätzlich vertraulich behandelt. Ausnahmen könnten zum Beispiel bei

berechtigter Annahme einer böswilligen Verleumdung oder Behauptung unwahrer Tatsachen bestehen. Im Einzelfall würde immer eine Abwägung gemäß § 22 Abs. 2 Nr. 2 HDSIG erfolgen.

§ 22 Abs. 2 HDSIG

(1) [1]Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden. 2Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. 3Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 21 zulässig.

(2) [1]Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht öffentliche Stellen ist zulässig, wenn

1. *sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden,*
2. *der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder*
3. *es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist*

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. [2]Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

Die ordnungsgemäße Abwägung der Interessen der Beteiligten habe im vorliegenden Fall zu Lasten des Betroffenen geführt.

Die Darstellung des Sozialamtes warf für mich weitere Fragen auf:

– Warum hatte das Sozialamt wegen eines anonymen Hinweises unmittelbar die Einstellung der SGB XII-Leistungen des Betroffenen veranlasst?
– Warum wurde, nach dem Grundsatz der Direkterhebung, der Betroffene nicht kontaktiert und mit dem Hinweis konfrontiert?
– Weshalb wurde der anonyme Hinweis sofort als glaubhaft und zweifelsfrei bewertet, so dass der Erlass eines Bescheides auf Einstellung der Leistung zwingend geboten schien?

In seiner zweiten Stellungnahme räumte das Sozialamt ein, dass der/die Verfasser/in des Hinweisschreibens der Behörde persönlich bekannt sei und als vertrauenswürdig gelte.

Der Hinweis sei zutreffend gewesen, da festgestellt werden konnte, dass sich der Betroffene tatsächlich nicht mehr in Deutschland aufhalte. Das Bekanntsein der hinweisgebenden Person beim Sozialamt ändere nichts am Ergebnis der Interessenabwägung, die Information über die Person nicht an den Betroffenen weiterzugeben. Die Datenschutzinteressen des Betroffenen seien nicht verletzt worden. Ein finanzieller Nachteil sei ebenfalls nicht entstanden, da die Leistungen rechtzeitig wieder angewiesen worden seien.

Rechtliche Bewertung

Tatsächlich ist es so, dass manche Teile der öffentlichen Verwaltung auch auf Hinweise der Bevölkerung angewiesen sind, um möglichen Missständen, Rechtsverstößen oder Ähnlichem nachgehen zu können. Damit wird kein mutwilliges Denunziantentum befördert oder dazu aufgerufen, irgendwelche Verleumdungen und dergleichen bei Behörden abzugeben.

Geht ein solcher unaufgeforderter Hinweis bei einer Behörde ein, so hat diese nach pflichtgemäßem Ermessen und im Rahmen ihres Amtsermittlungs- bzw. Untersuchungsgrundsatzes zu prüfen, ob sie den Informationen einen glaubhaften Wahrheitswert beimisst, und, bejahendenfalls, diesen nachzugehen. Dagegen bestehen keine datenschutzrechtlichen Einwände.

Grundsätzlich haben Sozialleistungsträger jedoch stets das datenschutzrechtliche Prinzip der Direkterhebung, § 37 S. 3 SGB I und § 67a Abs. 2 S. 1 SGB X, zwingend zu beachten.

§ 37 S. 3 SGB I

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

§ 67a Abs. 2 S. 1 SGB X

(2) [1] Sozialdaten sind bei der betroffenen Person zu erheben.

Im vorliegenden Fall konnte die Sozialbehörde den Betroffenen in der gebotenen Zeit allerdings nicht unmittelbar kontaktieren, da der Betroffene nach dortiger Überzeugung bereits im Ausland weilte. Um eine Überzahlung von Leistungen oder eine unrechtmäßige Auszahlung von Sozialleistungen, auf die tatsächlich kein Anspruch mehr besteht, rechtzeitig zu vermeiden, sah sich das Sozialamt genötigt, den Bescheid über die Einstellung von Sozialleistungen ab dem Folgemonat zu erlassen. Um die Rechte des Betroffenen dennoch soweit möglich zu wahren, hat man ihm die Möglichkeit eingeräumt,

seine (rechtzeitige) Rückkehr nach Deutschland nachzuweisen bzw. in diesem Zusammenhang seinen weiteren, durchgehenden Anspruch auf Leistungen nach dem SGB XII geltend zu machen. Dementsprechend wurde die Leistung ohne finanziellen Nachteil wieder fortgesetzt.

Aufgrund dieser speziellen Konstellation konnte ich im vorliegenden Fall – insbesondere wegen der sich zeitlich überschneidenden Abläufe – einen eindeutigen Verstoß gegen sozialdatenschutzrechtliche Vorschriften durch das Sozialamt nicht feststellen.

Allerdings habe ich das Sozialamt daraufhin gewiesen, dass die Nichtbefolgung des Direkterhebungsgebotes nur ein Ausnahmefall sein kann und darf.

Betroffenen ist Gelegenheit zu geben, sich zu (auch behördlicherseits als glaubhaft eingestuften) Vorwürfen und Hinweisen gegen ihre Person zu äußern. Der Erlass eines Bescheides allein mit Bezug auf einen „glaubhaften" Wahrheitsgehalt eines Hinweises kann in der Regel nicht akzeptiert werden.

6.4
Neues Bundesteilhabegesetz: Sozialdatenschutz im trägerübergreifenden Reha-Prozess

Im Rahmen des Projektes „Datenschutz im trägerübergreifenden Reha-Prozess" bei der Bundesarbeitsgemeinschaft für Rehabilitation (BAR) in Frankfurt am Main war ich als Vertreter der Bundesländer Mitglied einer Projektgruppe zur Ausarbeitung einer Arbeitshilfe zu o. g. Thema. Rechtlicher Hintergrund für das Bestreben nach einer solchen Arbeitshilfe war die Neustrukturierung des SGB IX im Zuge des Bundesteilhabegesetzes (BTHG). Das Projekt konnte im Sommer 2019 mit einem guten Ergebnis beendet werden.

Im Sommer 2018 trat die BAR über den Vorsitz der Datenschutzkonferenz auf die Datenschutzaufsichtsbehörden mit dem Wunsch zu, für ein dort geplantes Projekt zur Erstellung einer Arbeitshilfe mit dem Projekttitel „Datenschutz im trägerübergreifenden Reha-Prozess" mindestens eine/n Teilnehmer/-in aus dem Kreis der Landesdatenschutzaufsichtsbehörden als ständiges und aktives Mitglied zu werben und gewinnen zu können. Dies erschien der BAR aus nachvollziehbaren Gründen sinnvoll, um neben dem Vertreter des Bundesdatenschutzbeauftragten (BfDI) als zuständiger Datenschutzaufsichtsbehörde auch noch eine/-n Teilnehmer/-in aus dem Kreis der Landesdatenschutzaufsichtsbehörden gewinnen zu können, da das BTHG / SGB IX-neu Breitenwirkung haben werde. Ich habe diese Aufgabe gerne übernommen und nahm in der Folge als einvernehmlich beauftragter Vertreter

der Landesdatenschutzbeauftragten als Mitglied der o. g. Projektgruppe an den Sitzungen im Jahr 2019 teil.

Neben dem BfDI, HBDI und Vertretern der BAR waren weitere Teilnehmer/Mitglieder dieser Projektgruppe Vertreter/-innen von:

– Bundesministerium für Arbeit und Soziales
– Bundesministerium für Gesundheit
– Deutsche Rentenversicherung Bund
– Deutsche Gesetzliche Unfallversicherung (DGUV)
– Bundesagentur für Arbeit
– GKV-Spitzenverband
– Sozialversicherung für Landwirtschaft, Forsten und Gartenbau
– für die Bundesländer: Ministerium für Arbeit, Gesundheit und Soziales NRW
– für die Integrationsämter: Zentrum für Familie und Soziales Bayern

An insgesamt sechs Terminen vor Ort bei der BAR in Frankfurt am Main wurde in ganztägigen Arbeitssitzungen das Projektthema auf- und ausgearbeitet.

In der letzten Sitzung der Projektgruppe konnte konsensual die *Arbeitshilfe „Datenschutz im trägerübergreifenden Reha-Prozess“* verabschiedet werden. Diese Arbeitshilfe stellt natürlich einen Kompromiss der unterschiedlichsten Belange und (fachlichen) Anforderungen der beteiligten Institutionen dar. So konnten auch BfDI und HBDI in durchaus erfreulichem Sinn Einfluss nehmen und ein angemessenes Ergebnis erzielen.

Die Arbeitshilfe steht auf der Internetpräsenz der BAR zum Download bereit und kann von dort auch als gebundene Broschüre bezogen werden.

Seitens der BAR ist ab Winter 2019 ein an das Projekt anknüpfendes bzw. dieses vertiefendes Folgeprojekt „Datenschutz in der Rehabilitation“ geplant. Hier werden sich voraussichtlich der gleiche Institutions- und Teilnehmerkreis wieder einbringen und ein für die Praxis hilfreiches Dokument erarbeiten.

7. Schulen, Hochschulen, Statistik

7.1
Das Lehrerbildungsgesetz bedarf verbindlicher Datenverarbeitungsnormen

Das hessische Lehrerbildungsgesetz regelt die Ausbildung von Lehramtsabsolventen im Vorbereitungsdienst bzw. Referendariat. Bislang sind in diesem Gesetz Normen hinsichtlich der Verarbeitung personenbezogener Daten der Studierenden nur unzureichend vorhanden. Fast zwei Jahre nach Geltungsbeginn der Datenschutz-Grundverordnung ist es Zeit, klare Regelungen zu schaffen.

Das hessische Lehrerbildungsgesetz (HLbG, GVBl. I 2011 S. 590) regelt die Ausbildung und Prüfung von Lehramtsanwärterinnen und Lehramtsanwärtern. Das Gesetz enthält vielfältige Normen hinsichtlich des Studiums und der Praktika, der ersten und zweiten Staatsprüfung oder der Lehrbefähigung und der Unterrichtsbefugnis. Nähere Ausführungen hierzu sowie Regelungen hinsichtlich der pädagogischen Ausbildung sind in der Verordnung zur Durchführung des Hessischen Lehrerbildungsgesetzes (HLbGDV vom 28.09.2011) enthalten. Die pädagogische Ausbildung erfolgt in den studierten Fächern an zehn Studienseminaren an 17 Standorten sowie an Ausbildungsschulen, die den Studienseminaren regional zugeordnet sind.

Leider enthalten beide Rechtsnormen kaum Vorschriften zum Umgang und der Verarbeitung personenbezogener Daten der Lehramtsanwärterinnen und Lehramtsanwärter. Dies ist jedoch gerade im Hinblick darauf, dass die Datenschutz-Grundverordnung seit annähernd zwei Jahren Gültigkeit hat, ein Zustand, der dringend einer Änderung bedarf. Schließlich werden derzeit von weit mehr als 1.000 angehenden Lehrer*innen personenbezogene Daten erhoben und verarbeitet.

Im Rahmen der Ausgestaltung von Normen halte ich es für dringend geboten, das sog. Homogenitätsprinzip zu beachten. Die Datenverarbeitung nur in einer Verordnung Regeln zu wollen, genügt diesen Anforderungen nicht. Inhalt, Zweck und Ausmaß müssen vielmehr im Gesetz bestimmt werden. Ist durch ein Gesetz vorgesehen, dass eine Ermächtigung weiter übertragen werden kann, so bedarf es zur Übertragung der Ermächtigung einer Rechtsgrundlage. Das ist im Regelfall eine Rechtsverordnung.

So wie im Hessischen Schulgesetz grundsätzliche Bestimmungen zur Verarbeitung personenbezogener Daten der Schülerinnen und Schüler, Lehrkräfte und Eltern enthalten sind und die konkrete Ausgestaltung in der Verordnung zur Verarbeitung personenbezogener Daten in Schulen erfolgt,

sind grundsätzliche Datenverarbeitungsnormen in das Lehrerbildungsgesetz aufzunehmen. Die konkrete Ausgestaltung ist dann in der bereits bestehenden Verordnung zur Durchführung des Lehrerbildungsgesetzes umzusetzen.

7.2
Menschliches Versagen und unzureichende organisatorisch-administrative Maßnahmen führten an dem Institut für Berufsbildung (IBB) der Universität Kassel zu einem gravierenden datenschutzrechtlichen Verstoß.

Das IBB der Universität Kassel nutzt zur Entsorgung von Papieren und Unterlagen mit personenbezogenen Daten abschließbare Container, die ein externer Dienstleister zur Verfügung stellt. Die Container werden innerhalb vereinbarter Zeiträume abgeholt und die personenbezogenen Dokumente datenschutzgerecht vom Entsorger vernichtet. Um versehentlichen eingeworfene Unterlagen wieder herausholen zu können, wurden in dem Institut mehrere Schlüssel für die Container vorgehalten. Eine neue Mitarbeiterin im Sekretariat nutzte diese Möglichkeit. Fatal allerdings war, dass sie den geöffneten Container nicht wieder abschloss. Vielmehr wurde der Container an einer anderen Stelle platziert, nämlich auf einen Gang innerhalb des Institutsbereichs, in dem regelmäßiger Publikumsverkehr herrschte. Kein Wunder also, dass binnen kurzer Zeit jemand Interesse an dem deplatziert wirkenden Container fand und feststellte, dass dieser nicht verschlossen war.

Im Container befanden sich personenbezogene Daten u. a. von Lehramtsanwärterinnen und Lehramtsanwärtern. Meine Dienststelle wurde anonym über die Datenpanne informiert. Der E-Mail beigefügt waren eine Vielzahl von Bilddateien, welche die Qualität der ungeschützten und eigentlich zur Vernichtung vorgesehenen Dokumente zeigten. Dabei handelte es sich u. a. um

- Listen mit Namen, Schule, Matrikel-Nummer sowie private E-Mail-Adressen und Telefonnummern,
- Bestätigungen über den Empfang eines Merkblattes zur Umsetzung des
- Infektionsschutzgesetzes mit Namen und Geburtsdatum,
- Teilnehmerlisten an einem Kurs des Wintersemesters 2016/17,
- Praktikumsbescheinigung einer Lehramtskandidatin,
- Inhaltsverzeichnis zum Bericht mit persönlichen Anmerkungen zu einem Schüler,
- schriftliche Erklärung zu einer Hausarbeit u. a.

Maßnahmen der Universität Kassel

Nachdem ich die Universitätsleitung auf die Datenpanne hinwies, reagierte sie schnell und schaltete auch die Datenschutzbeauftragten der Hochschule ein. Der Container wurde unverzüglich wieder verschlossen und an seinen ursprünglichen Standort verbracht.

Bei der Aufarbeitung der Panne wurde alsbald deutlich, dass der Vertrag zur Auftragsverarbeitung (Art. 28 DS-GVO) sowie die interne Organisation der Schlüsselberechtigung und Schlüsselverwahrung einer Nachbesserung bedurfte. Wie sich herausstellte, war nicht klar, wie viele Schlüssel überhaupt in Umlauf waren, wo diese aufbewahrt werden und wer auf sie Zugriff hatte. Folglich mangelte es auch an der Zuordnung der Verantwortung für die einzelnen Schlüssel. Künftig wird es nur noch einen Schlüssel geben, der an einer sicheren Stelle aufbewahrt und verwaltet wird. Die Mitarbeiterinnen und Mitarbeiter wurden entsprechend sensibilisiert. Derartige Regelungen gehören zu den technischen und organisatorischen Sicherheitsmaßnahmen, die jeder Verantwortliche einer Datenverarbeitung zu treffen hat, um ein angemessenes Schutzniveau für die von ihm verarbeiteten Daten zu gewährleisten (Art. 32 DS-GVO).

In diesem Fall eigentlich eine ziemlich einfache Sache, so etwas zu regeln. Dennoch bedurfte es erst dieser Datenpanne, um eine Verfahrensweise festzulegen, die es eigentlich von vornherein hätte geben müssen. Eine Meldung nach Art. 33 DS-GVO war nicht erforderlich, da der Universitätsverwaltung die Datenschutzverletzung erst durch meine Information bekannt wurde und sie dann unverzüglich alle erforderlichen Maßnahmen umsetzte.

7.3
Das Hessische Schulportal entwickelt sich

Bereits im Jahr 2016 haben sich die Bildungsminister der Länder mit ihrer gemeinsamen Strategie „Bildung in der digitalen Welt“ auf klare Ziele und Zeithorizonte hinsichtlich des Einsatzes von sog. Learning Management Systemen (LMS) oder auch Lernplattformen festgelegt. In Hessen wird eine landeseinheitliche Lernplattform in Rahmen des sogenannten Schulportals umgesetzt.

Die Vorteile von digitalen Plattformen

Die Vorteile liegen auf der Hand. Schule ist nicht mehr allein der Ort, an dem durch Lehrkräfte z. B. Aufgaben für Schülerinnen und Schüler gestellt oder Lehr- und Lernmaterialien zur Verfügung gestellt werden. Die physische Präsenz aller Akteure wird zum Teil entbehrlich, weil die Daten in eine Cloud

transportiert werden, auf welche die Betroffenen einen Zugriff haben. Auch zur Kommunikation können solche Systeme eingesetzt werden und damit die Funktionalität derartiger Plattformen erweitern. Schließlich ist auch Schulorganisation auf diese Weise möglich, weil Raumpläne oder Stundenplanänderungen über das Medium kommuniziert werden. Eine Reihe von Bundesländern hat sich für landeseinheitliche digitale Plattformen entschieden. In Nordrhein-Westfalen z. B. war dies „logineo“, in Baden-Württemberg eine Plattform namens „ella“. Niedersachsen und Bayern setzen ebenfalls zentrale Lösungen ein oder arbeiten daran. Auch in Hessen macht die Entwicklung einer zentralen Portallösung Fortschritte.

Das hessische Schulportal wird Schritt für Schritt aufgebaut

Seit Jahren arbeiten Mitarbeiter der Hessischen Lehrkräfteakademie mit Unterstützung und nach den Vorgaben des zuständigen Digitalisierungsreferats im Hessischen Kultusministerium an der Entwicklung eines Portals, das sich insbesondere dadurch auszeichnet, dass ausschließlich „Freeware“-Software zum Einsatz kommt. Die Bindung an spezifische Produkte bestimmter Hersteller entfällt damit. Abgeordnete Lehrkräfte mit Praxiswissen aus dem Schulalltag entwickeln sowohl Anwendungen für den pädagogischen Bereich als auch für die Schulorganisation. So steht beispielsweise die Funktionalität eines elektronischen Notenbuchs für die Lehrkräfte im sog. LANiS zur Verfügung. Der Name ist ein Akronym und steht für „**L**eichte **A**dministration von **N**etzwerken **i**n **S**chulen“). Damit werden Zugänge und Anwendungen für Schülerinnen und Schüler sowie Lehrkräfte organisiert.

Mittlerweile sind eine ganze Reihe von Anwendungen hinzugekommen, die in einer geschlossenen Plattform allen Beteiligten zur Verfügung steht. Etwa ein Viertel aller hessischen Schulen sind derzeit am Schulportal angemeldet, etwa 250 von diesen Schulen nutzen die Anwendungen umfangreich. Weitere Module wie z. B. Ablagemöglichkeiten von Unterrichtsmaterial sind in Planung oder auch teilweise bereits realisiert.

Datenschutzrechtliche Aspekte bei der Nutzung durch Schulen

In aller Regel werden im Rahmen der Nutzung von digitalen (Lern-)Plattformen personenbezogene Daten der Lehrkräfte und Schülerinnen und Schüler verarbeitet. Das beginnt mit der Einrichtung eines Accounts und setzt sich z. B. mit der Kommunikation fort. Auch die Vergabe von Hausarbeiten und deren Bewertung ist Bestandteil ihrer Funktionalität.

Den Schulen ist es nicht untersagt, digitale Lernmittel zu nutzen. Sie müssen jedoch die Teilhabe garantieren sowie für die Sicherheit der Datenverar-

beitung Sorge tragen. Schließlich ist die Schule bzw. die Schulleitung als Verantwortlicher im Sinne von Art. 24 DS-GVO für die datenschutzkonforme Verarbeitung der personenbezogenen Daten von Lehrkräften und Schülerinnen und Schülern in der Pflicht. Datenschutzrechtliche Anforderungen für die Nutzung von z. B. Lernplattformen haben die Datenschutzbeauftragten von Bund und Ländern in einer „Orientierungshilfe Lernplattformen“ (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Orientierungshilfe%20Online-Lernplattform%20im%20Schulunterricht%20-%20Stand%2004-2018.pdf) formuliert. Die Umsetzung dieser Anforderungen stellt Anbieter von Plattformen zum Teil vor große Herausforderungen. Dies gilt in gleichem Maße für Schulen, die mit den Werkzeugen für den Datenschutz und die Datensicherheit, die der Anbieter liefert, angemessen umgehen sollen. Je komplexer ein Verfahren ist und damit die Vielzahl der Funktionalitäten unübersichtlich wird, desto größer ist die Gefahr, dass im Rahmen der Anwendung grundsätzliche datenschutzrechtliche Fragestellungen unbeachtet bleiben.

Datenschutzrechtliche Anforderungen an das hessische Schulportal

Eine umfassende datenschutzrechtliche Bewertung des hessischen Schulportals habe ich bislang nicht vornehmen können, auch wenn es im Berichtsjahr eine Reihe von Kontakten und Austausch mit den zuständigen Vertretern der Lehrkräfteakademie gab. Dennoch habe ich gegenüber dem Hessischen Kultusminister meinen grundsätzlich positiven datenschutzrechtlichen Eindruck von der Plattform mitgeteilt. Gleichzeitig habe ich angekündigt, dass nur auf der Grundlage einer umfassenden Dokumentation eine qualifizierte Bewertung durch mich erfolgen kann.

Das Kernelement des Portals ist das zentrale Identitätsmanagement. Dies muss im Hinblick auf die favorisierte „Single-Sign-On“-Lösung im Rahmen des Zugangs hohen Ansprüchen genügen. Single-Sign-On ist sinnvoll, um den Zugang zum Portal nicht unverhältnismäßig komplex werden zu lassen. Aber auch Zugriffsberechtigungen, Protokollierung oder Authentifizierungsverfahren stehen im Focus der datenschutzrechtlichen Betrachtung. Nicht zuletzt sind Verzeichnisse von Verarbeitungstätigkeiten nach Art. 30 DS-GVO erforderlich, die derzeit von der Lehrkräfteakademie erstellt werden.

Gelingt es den Beteiligten, diese Herausforderungen zu bewältigen, stünde einem generellen Einsatz des Portals als einem hessenweiten Angebot an die Schulen nichts im Wege.

7.4
Technische Untersuchungen zum datenschutzkonformen Einsatz von Office 365 im pädagogischen Bereich hessischer Schulen

Seit Jahren befasse ich mich mit dem Thema eines datenschutzkonformen Einsatzes der Anwendung Office 365 im schulischen Bereich. Auch im Berichtsjahr habe ich mit hohem Aufwand bestimmte Produktlinien von Office 365 geprüft. Vorläufiges Resultat dieser Prüfungen waren zwei Stellungnahmen mit dem Ziel, aufgrund nachhaltiger Erkenntnisse zu einer endgültigen Bewertung kommen zu können. Die bislang erfolgten technischen Inspektionen, insbesondere an Schulen vor Ort, werden fortgeführt.

Mit dem im Mai 2019 beschlossenen, bundesweiten Digitalpakt zur Modernisierung auch der hessischen Schulen ist der Einsatz der Anwendung Microsoft Office 365 im Lizenzmodell Microsoft Education verstärkt bei mir angefragt worden. Diese Produktlinie wurde innerhalb des Jahres fortlaufend – auch technisch – für den Einsatz an hessischen Schulen im pädagogischen Bereich geprüft. Zwei Stellungnahmen meines Hauses führten zu direkten Gesprächen mit dem Hersteller Microsoft.

Eines verstärkten Prüfbedarfs einerseits und Gesprächen unmittelbar mit Microsoft andererseits bedurfte es deshalb, weil im Berichtsjahr einzelne Schulträger (unabhängig datenschutzrechtlich offener Fragestellungen) Dienste, die mit Microsoft Office 365 verbunden sind, massiv in die Schullandschaft ausrollten. Für Verantwortliche wie Schulleitungen war es fast unmöglich einzuschätzen, welches Lizenzmodell ihren Bedarf abdeckt und gleichzeitig eine datenschutzkonforme Lösung darstellt. Insbesondere wird eine solche Entscheidungsfindung aus mehreren Gründen erschwert, weil nicht nur Applikationen und Dienste der Produktlinie Microsoft Education angeboten werden.

Aus technischer Sicht gelten für den Einsatz von Microsoft Office 365 die datenschutzrechtlichen Anforderungen für eine datenschutzkonforme Verarbeitung personenbezogener Daten, die sich aus den Art. 5, 25, 28, 32 und 46 DS-GVO ableiten oder die sich aus Entscheidungen des Europäischen Datenschutzausschusses, Untersuchungen des Europäischen Datenschutzbeauftragten, des IT-Planungsrates oder der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder ergeben.

Hinsichtlich des Einsatzes von Office 365 auf Basis Microsoft Education im pädagogischen Bereich hessischer Schulen wird aktuell die Rolle des Herstellers Microsoft im Verhältnis zu anderen Rechenzentren oder IT-Dienstleistern diskutiert.

7.5
Digitalisierung des Verfahrens der Schülerbeförderung

Der Schulträger des Kreises Groß-Gerau plant die Neugestaltung und Digitalisierung des Prozesses der Schülerbeförderung. Nach § 161 des Hessischen Schulgesetzes sind die Schulträger unter bestimmten Voraussetzungen zur Kostenerstattung gegenüber den Eltern verpflichtet. Der Kreis Groß-Gerau ist als bundesweit eine der ersten Einrichtungen dabei, im Sinne des Onlinezugangsgesetzes einen digitalen Prozess zu schaffen, der von der Beantragung bis hin zur Rückerstattung von Geld die Verwendung von Papier obsolet machen soll.

Das Onlinezugangsgesetz (OZG) verpflichtet Bund und Länder, bis spätestens 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Der Landkreis Groß-Gerau ist nun bundesweit einer der ersten Schulträger (die Stadt München bietet einen solchen Service seit Mitte 2018), der alle Leistungen rund um die Schülerbeförderung den Eltern in einem Online-Verfahren zur Verfügung stellen soll.

In diesem Zusammenhang ergeben sich datenschutzrechtliche Fragestellungen hinsichtlich der Sicherheit der Datenübermittlung, des Zugriffsschutzes oder der Datenspeicherung. Insbesondere muss bewertet werden, ob der erforderliche Zugriff auf die Lehrer- und Schülerdatenbank (LUSD), um die Angaben über die Schülerinnen und Schüler prüfen zu können, datenschutzrechtlich möglich ist. In der LUSD, einem gemeinsamen Verfahren der Schulen und des Hessischen Kultusministeriums, sind unter anderem die Stammdaten der Schülerinnen und Schüler gespeichert wie z. B. Name, Adresse oder Geburtsdatum. Bei einem automatisierten Abgleich mit den Daten der LUSD stellt sich die Frage, ob bei Feststellung einer Ungleichheit der abgefragten Daten mit denen der LUSD, z. B. wenn dort eine andere Adresse angegeben ist, diese abweichenden Daten an den Schulträger übermittelt werden dürfen.

Das Verfahren, das derzeit durch die Verantwortlichen modelliert wird, bedarf noch einer genaueren Betrachtung auf der Grundlage nachvollziehbarer Informationen.

Der Ansatz erscheint zum derzeitigen Zeitpunkt interessant und unter datenschutzrechtlichen Gesichtspunkten realisierbar zu sein. Ich werde deshalb das Verfahren weiterhin begleiten.

7.6
Der Zensus 2021 rückt näher

Im Jahr 2021 wird in Deutschland und EU-weit wieder ein registergestützter Zensus – eine Volks-, Gebäude- und Wohnungszählung – stattfinden. Mit dem Zensus sollen in Deutschland die amtliche Einwohnerzahl sowie eine Reihe von Daten zur Bevölkerung, Erwerbstätigkeit und der Wohnsituation erhoben werden. Der letzte Zensus wird dann zehn Jahre zurückliegen.

Rechtsgrundlage und beabsichtigtes Vorgehen

Die Durchführung des Zensus 2021 und insbesondere, welche Register bzw. Datenquellen hierfür genutzt werden, regelt das Gesetz des Bundes zur Durchführung des Zensus im Jahre 2021 (Zensusgesetz 2021) vom 26. November 2019.

Parallel hat der hessische Gesetzgeber ein „Hessisches Ausführungsgesetz zum Zensusgesetz 2021“ auf den Weg gebracht, das die Errichtung der örtlichen Erhebungsstellen bei den Landkreisen, den kreisfreien Städten und den Sonderstatusstädten sowie die Anforderungen an ihre Einrichtung und Leitung und die im Einzelnen wahrzunehmenden Aufgaben regelt.

Mit Stichtag 9. Mai 2011 wurde in Deutschland erstmals ein registergestützter Zensus durchgeführt. Der Zensus 2021 wird erneut eine registergestützte Erhebung sein.

Eine der von der amtlichen Statistik beim Zensus 2011 gewonnenen Erkenntnisse war der Umstand, dass die genutzten Register teilweise nicht den erforderlichen Qualitätsansprüchen genügten. Die Konsequenz daraus war der Aufbau eines anschriftenbezogenen Steuerungsregisters, in dem alle Anschriften mit Wohnraum und Angaben zu den Gebäude- und Wohnungseigentümern hinterlegt sind. Die Daten erhielten die Statistiker vom Amtlichen Liegenschaftskatasterinformationssystem (ALKIS) aus den Melderegistern der Meldebehörden sowie Vermessungsdaten des Bundesamtes für Kartografie und Geodäsie (BKG).

Auf Grundlage dieser Daten wird eine Totalerhebung der Gebäude- und Wohnungseigentümer (GWZ) durchgeführt. Zudem erfolgt eine Haushaltebefragung auf Basis einer Stichprobe, die bei etwa zehn Prozent liegt. Außerdem ist im Rahmen der Qualitätssicherung eine Wiederholungsbefragung vorgesehen.

Die Datenverarbeitung erfolgt in verschiedenen IT-Systemen und Fachanwendungen. Im Rahmen der „Online-First“-Strategie der amtlichen Statistik sollen die Antworten aus der Gebäude- und Wohnungszählung durch die Auskunftspflichtigen primär online abgegeben werden. Hierzu wurde, wie im Jahr 2011, ein Online-Portal aufgebaut. Die Daten werden innerhalb einer

Fachanwendung verarbeitet. Dies gilt gleichfalls für die Haushaltestichprobe. Über einen Referenzdatenbestand (dem Steuerungsregister) erfolgt der Abgleich und die Plausibilisierung der Datenbestände.

Bei den technischen Prozessen der Datenverarbeitung kommt dem Statistischen Bundesamt bzw. seinem Auftragsverarbeiter, dem Informationstechnikzentrum Bund (ITZBund), eine zentrale Bedeutung zu. Anders noch als beim Zensus 2011 verarbeiten die Länder die Daten ihres jeweiligen Zuständigkeitsbereichs nicht selbst, sondern sind den Verfahren beim ITZBund durch eine Verwaltungsvereinbarung angeschlossen. Die zentrale Datenhaltung auf Informationssystemen des Bundes und die Reduzierung der Befugnisse der Länder auf „ihre" Daten in Form von „Zugriffen" oder „Abrufen" stellt eine – auch datenschutzrechtliche – Besonderheit dar, für die es bislang kein Beispiel gibt.

Datenschutzrechtliche Fragestellungen

Aus der geschilderten DV-gestützten Konstruktion, die in dieser Form erstmals zur Anwendung kommt, ergeben sich Fragen hinsichtlich der Verantwortlichkeit. Für die zentrale IT-Infrastruktur sowie die Sicherheit der Datenverarbeitung liegt die Verantwortung gem. Art. 24 DS-GVO beim Statistischen Bundesamt. Dies gilt auch für die Umsetzung der erforderlichen Maßnahmen zur Datensicherheit i. S. v. Art. 32 DS-GVO. Für die Zugriffe oder Abrufe sind die Statistischen Landesämter der Länder bzw. die Erhebungsstellen verantwortlich.

Der Schutzbedarf der personenbezogenen Meldedaten ist als „sehr hoch" zu bewerten. Dies liegt zum einen darin begründet, dass in den Melderegistern auch Daten von Personen enthalten sind, für die eine sog. „Auskunftssperre" gilt. Dabei handelt es sich z. B. um gefährdete Personen wie z. B. Personen, die die Androhung von Gefahr für Leib und Leben glaubhaft machen konnten, oder Personen, die sich in einem Zeugenschutzprogramm befinden. Zum anderen wäre es möglich, Personen über deren Namen und Geburtsdatum zu identifizieren und deren Anschrift zu ermitteln. Aus den nach § 5 des Zensusgesetzes an die amtliche Statistik zu übermittelnden Personendaten ergibt sich daher der sehr hohe Schutzbedarf. Entsprechend nachvollziehbar und sicher müssen die Datenverarbeitungsprozesse gestaltet sein. Die zur datenschutzrechtlichen Bewertung erforderlichen Informationen sollen den Aufsichtsbehörden für den Datenschutz, so auch meiner Behörde, zeitnah zur Verfügung gestellt werden.

Auftragsverarbeitung durch die Statistischen Landesämter

Außer den Ländern Nordrhein-Westfalen, Niedersachsen, Baden-Württemberg und Bayern haben sich die Statistikämter der Länder zu einem Verbund zusammengeschlossen. Innerhalb des Verbundes werden zentrale Verfahren gemeinsam ausgeschrieben und realisiert. Zuletzt stand die Vergabe der Dienstleistungen Druck der Erhebungspapiere der Gebäude- und Wohnungszählung sowie der Telefon-Hotline an. Anders als 2011 beabsichtigt das Hessische Statistische Landesamt, kein eigenes Call-Center für den Zensus 2021 zu betreiben, sondern ein externes Unternehmen damit zu beauftragen. Auch hierzu ergeben sich datenschutzrechtliche Fragen. So bedarf es z. B. der Klärung, ob und in welchem Umfang die externen Kräfte mit einem Auskunftspflichtigen inhaltliche Fragen des Bogens besprechen und für diesen ausfüllen dürfen. Welche Art von Zugriffs- und Schreibberechtigungen wären hierfür erforderlich? Dürften derartige hoheitliche Maßnahmen von einem externen Dritten überhaupt ausgeführt werden?

Diese und eine Vielzahl weiterer Fragen werden im kommenden Berichtsjahr einer weiteren Klärung bedürfen. Dabei ist eine vertrauensvolle Zusammenarbeit mit dem Hessischen Statistischen Landesamt eine wichtige Voraussetzung. Die seit Anfang des Jahres erfolgten regelmäßigen Kontakte waren bislang eine gute Grundlage, um den Prozess rund um den Zensus 2021 datenschutzrechtlich angemessen begleiten zu können. Die Aufsichtsbehörden von Bund und Ländern sind in den kommenden Jahren gefordert, das Datenverarbeitungs-Großprojekt Zensus 2021 in puncto Datenschutz kritisch und konstruktiv im Interesse der Bürgerinnen und Bürger zu begleiten.

8. Verkehr, Daseinsvorsorge

8.1
Ausweis- und Führerscheinkopien bei Probefahrten von Kaufinteressenten

Die Erhebung von Ausweis- und Führerscheindaten ist für Probefahrten von Kaufinteressenten erforderlich. Aufgrund des Grundsatzes der Datenminimierung sollte jedoch auf das Anfertigen entsprechender Kopien verzichtet werden.

Im Berichtszeitraum erhielt ich eine Beschwerde gegen ein Autohaus, das zur Durchführung von Probefahrten Kopien der Personalausweise und der Führerscheine der Kaufinteressenten anfertigte.

Vorlage des Führerscheins und Feststellung der Identität

Außer Zweifel steht, dass das Vorlegen einer gültigen Fahrerlaubnis sowie die Angabe der Personalien durch das Autohaus bei Durchführung einer Probefahrt aufgrund der dem Händler obliegenden Sorgfaltspflichten und strafrechtlichen Vorschriften verlangt werden können.

Das Autohaus hat als Halter des Fahrzeugs Sorge dafür zu tragen, dass ein Fahrzeug nur von Personen geführt wird, die die dazu erforderliche Fahrerlaubnis vorweisen können. Unterlässt der Händler diese Prüfung, kann dies für ihn nicht nur strafrechtliche Konsequenzen gemäß § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz (StVG), sondern auch versicherungsrechtliche Auswirkungen haben. Entstehen durch die Probefahrt beispielsweise Schäden am versicherten Fahrzeug, kann der Versicherer die Übernahme der Leistung verweigern, wenn der Halter entgegen D 1.1.3 der Allgemeinen Bedingungen für die Kraftfahrzeugversicherung (AKP) zugelassen hat, dass ein Fahrer ohne erforderliche Fahrerlaubnis ein Fahrzeug auf öffentlichen Wegen und Plätzen führte.

Aber auch die Aufnahme der Personalien anhand des Personalausweises dient der Sicherung von versicherten Vermögenswerten und damit der Erfüllung der versicherungsrechtlichen Sorgfaltspflichten.

Die Überlassung des Fahrzeugs an einen Kaufinteressenten kann nämlich dann eine grob fahrlässige Ermöglichung der Entwendung gemäß § 81 des Versicherungsvertragsgesetzes (VVG) darstellen, wenn der Händler als Versicherungsnehmer Maßnahmen zur Feststellung der Identität des Kunden unterlässt und ihm das Fahrzeug zur Verfügung stellt (s. OLG Frankfurt am Main, Urteil vom 20.2.2002 - 7 U 54/01). In diesen Fällen kann die Versiche-

rung die Übernahme des durch einen Diebstahl des Fahrzeugs entstandenen Vermögensschadens verweigern oder kürzen, da der Versicherungsfall grob fahrlässig herbeigeführt wurde.

Für die Identitätsfeststellung fordert die Versicherungsbranche die Vorlage eines Personalausweises oder Reisepasses. Der Personalausweis und der Reisepass stellen amtliche Urkunden dar, mit der in Deutschland die Identität des Inhabers zweifellos festgestellt werden kann. Er enthält eine Vielzahl von Sicherheitsmerkmalen, mit denen die Echtheit überprüft werden kann.

Anfertigung der Kopie eines Personalausweises

Gemäß § 20 Abs. 2 Personalausweisgesetz (PAuswG) darf ein Personalausweis nur mit Einwilligung des Ausweisinhabers durch eine andere Person abgelichtet werden, wenn mit der Kopie personenbezogene Daten erhoben oder verarbeitet werden. Die Kopie muss als solche dauerhaft erkennbar sein. Im Übrigen sind die Vorschriften des allgemeinen Datenschutzrechts anzuwenden.

§ 20 Abs. 2 PauswG

(2) 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 datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Das Bundesministerium des Inneren hat mit Erlass vom 29.03.2011 u. a. weitere datenschutzrechtlich relevante Präzisierungen festgelegt, an denen ich die Zulässigkeit, einen Personalausweis zu kopieren, festmache. Danach muss der Ausweisinhaber auf die Möglichkeit der Schwärzung der für die Identifizierung nicht benötigten Daten hingewiesen werden. Ferner ist die Kopie vom Empfänger unverzüglich zu vernichten, sobald der verfolgte Zweck erreicht wurde.

Im Hinblick auf diese Vorschrift machte ich das betreffende Autohaus darauf aufmerksam, dass eine datenschutzrechtlich wirksame Einwilligung, eine Kopie zu fertigen, nur vorliegen kann, wenn Betroffene die Einwilligung freiwillig abgeben und über die Datenverarbeitung ausreichend informiert sind. Freiwilligkeit ist anzunehmen, wenn Betroffene eine ernsthafte Wahl haben,

wie z. B. zwischen der Kopie des Ausweises oder der schriftlichen Übernahme der erforderlichen Ausweisdaten in ein Formular entscheiden zu können.

Zu diesem Zeitpunkt verwendete das Autohaus ein von seinem Verband zur Verfügung gestelltes Formular, das weder die Möglichkeit bot, anstelle der Kopie die Daten schriftlich einzufügen, noch eine Datenschutzinformation nach Art. 13 DS-GVO enthielt. Als Alternative zur Einwilligung in das Kopieren des Ausweises blieb so nur der Verzicht auf die Probefahrt. Da dieses Formular als Muster von einem für das Kraftfahrzeuggewerbe zuständigen größeren Verband erstellt wurde, nahm ich mit diesem Kontakt auf und erwirkte eine entsprechende Überarbeitung.

Inzwischen veröffentlichte der Verband ein neues Formular, in dem zwischen der Kopie des Führerscheins und der schriftlichen Übernahme der Führerscheindaten ausgewählt werden kann. Ferner werden im Formular nur noch die Ausweisnummer, das Ausstellungsdatum und die Ausstellungsbehörde aus dem Personalausweis oder dem Reisepass zur Identifizierung schriftlich abgefragt. Des Weiteren enthält das Formular eine Muster- Datenschutzinformation nach Art. 13 DS-GVO, die durch den jeweiligen Benutzer (Autohaus) entsprechend anzupassen ist.

Im Sinne der Datenminimierung und der Datensparsamkeit wird von dem Verband zudem allgemein in einem Begleitschreiben empfohlen, die Datenerhebung mittels schriftlicher Übernahme vorzunehmen und von der Anfertigung von Kopien abzusehen. Entscheidet sich ein Autohaus dennoch, die Anfertigung von Ausweiskopien den Kaufinteressenten zur Wahl zu stellen, ist diese nur mit einer freiwilligen datenschutzrechtlichen Einwilligung und der Einhaltung gesetzlicher Vorschriften zulässig.

Das betroffene Autohaus versicherte, zukünftig das neue Formular bei Durchführung einer Probefahrt von Kaufinteressenten zu verwenden und die erforderlichen Daten nur noch im Formular einzutragen.

8.2
Datenverarbeitung von Funkrauchwarnmeldern

Für den Einsatz von Funkrauchwarnmeldern finden datenschutzrechtliche Vorschriften Anwendung, da die Fehlalarme des Rauchwarnmelders auf ein bestimmtes Verhalten der Bewohner schließen lassen und somit ein Personenbezug herstellbar ist.

Aufgrund einer Vielzahl von Beschwerden habe ich mich im Berichtszeitraum mit der Datenverarbeitung von Funkrauchwarnmeldern beschäftigt.

Seit Juni 2005 müssen bewohnte Immobilien in Hessen gemäß § 14 Abs. 2 Nr. 1 Hessische Bauordnung (HBO) mit Rauchwarnmeldern in allen Schlafräumen, Flucht- und Rettungswegen ausgestattet sein.

§ 14 Brandschutz

(1) Anlagen sind so anzuordnen, zu errichten, zu ändern und instand zu halten, dass der Entstehung eines Brandes und der Ausbreitung von Feuer und Rauch (Brandausbreitung) vorgebeugt wird und bei einem Brand die Rettung von Menschen und Tieren sowie wirksame Löscharbeiten möglich sind.

(2) Zum Schutz von schlafenden Personen müssen

1. *in Wohnungen die Schlafräume und Kinderzimmer sowie Flure, über die Rettungswege von Aufenthaltsräumen führen,*
2. *in sonstigen Nutzungseinheiten die Aufenthaltsräume, in denen bestimmungsgemäß Personen schlafen,*

jeweils mindestens einen Rauchwarnmelder haben. Die Rauchwarnmelder müssen so eingebaut oder angebracht und betrieben werden, dass Brandrauch frühzeitig erkannt und gemeldet wird. Die Sicherstellung der Betriebsbereitschaft obliegt

1. *in Wohnungen nach Satz 1 Nr. 1 den unmittelbaren Besitzerinnen und Besitzern,*
2. *in Nutzungseinheiten nach Satz 1 Nr. 2 den Betreiberinnen und Betreibern,*

es sei denn, die Eigentümerinnen oder die Eigentümer haben diese Verpflichtung übernommen. Bestehende Nutzungseinheiten nach Satz 1 Nr. 2 sind bis zum 1. Januar 2020 entsprechend auszustatten.

Bei der Planung, dem Einbau, dem Betrieb und der Instandsetzung von Rauchmeldern sind ferner die Anforderungen der Anwendungsnorm DIN 14676 zu beachten. So bestimmt die DIN 14676 beispielsweise, dass die Rauchwarnmelder in der Raummitte mit einem Mindestabstand von 50 cm zu einer Wand bzw. zu Einrichtungsgegenständen an der Decke anzubringen sind. Der Funkrauchwarnmelder muss einen Alarm absetzen, wenn er demontiert oder der 50 cm- Abstand nicht eingehalten wird. Der empfohlene Inspektionszyklus beträgt unabhängig von der Art des eingesetzten Rauchwarnmelders 12 Monate.

Dabei hängt der uneingeschränkte Versicherungsschutz des Gebäudes meist von dem Nachweis der ordnungsgemäßen Wartung der Rauchwarnmelder nach den maßgeblichen DIN-Vorschriften ab.

Die Eigentümer von vermieteten Wohnräumen können die Verpflichtung zur Sicherstellung der Betriebsbereitschaft nach § 14 HBO übernehmen. Von der Möglichkeit der Übernahme machen die Eigentümer vielfach zum Schutze ihres vermieteten Eigentums Gebrauch. Zur Erfüllung dieser Verpflichtung entscheiden sie sich immer häufiger für die Rauchwarnmelder mit Funkmodul. Diese bieten die Möglichkeit der kompletten Ferninspektion unter Einsatz

der Funktechnik an. Das Betreten der Wohnung ist nicht erforderlich. Das Betreten des Treppenhauses ist zur Erhebung der Daten ausreichend.

So wunderten sich die über den Einsatz der Funktechnik nicht informierten Mieter, wenn sie einen Brief vom Vermieter bekommen haben, mit der Aufforderung, den während der Renovierungsarbeiten demontierten Rauchwarnmelder wieder anzubringen. Deswegen beschwerten sich auch viele betroffene Mieter bei mir.

Diese Beschwerden habe ich zum Anlass genommen, die Funktionsweise von Funkrauchwarnmeldern bei einem im Hessen ansässigen Dienstleister näher zu betrachten. Dieser Dienstleister wird von den Vermietern /Hausverwaltungen mit Einbau, Inspektion, Instandsetzung und Dokumentation der Rauchwarnmelder beauftragt. Die Art der Rauchwarnmelder bestimmt dabei immer der Vermieter. Dabei kann er sich auch für die funkbasierte Technik entscheiden (so Bundesgerichtshof in seinem Urteil vom 17.06.2015 (VIII ZR 216/14)).

Bei meiner datenschutzrechtlichen Prüfung stellte ich fest, dass die Funkrauchwarnmelder eine Seriennummer (Baureihe) und ID (Gerätenummer) besitzen. Diese werden der jeweiligen Wohneinheit und dem Zimmer zugeordnet. Durch die Ferninspektionen können neben den technischen Werten (Batterieladezustand, technische Fehlfunktionen der Rauchsensorik oder des Warnsignals usw.) auch das Verhalten der Bewohner – die Demontage oder das Verstellen des Rauchwarnmelders – mithilfe der Funktechnik detektiert werden. Somit handelt es sich um personenbezogene Daten der Bewohner in Sinne des Art. 4 Nr. 1 DS-GVO.

Bei der automatisierten Verarbeitung von personenbezogenen Daten sind die Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes zu beachten. Die datenschutzrechtliche Grundlage für die Erhebung von personenbezogenen Daten stellt Art. 6 Abs. 1 S. 1 lit. c DS-GVO, § 14 HBO in Verbindung mit den Anforderungen der DIN 14676 dar. Durch die Anforderungen der DIN 14676 wird dabei der Stand der Technik festgelegt.

Weder der geprüfte Dienstleister noch die betroffenen Hausverwaltungen gingen beim Einsatz der Funkrauchwarnmelder von einer Verarbeitung personenbezogener Daten aus. Aufgrund meines Prüfungsergebnisses hat der Dienstleister zugesichert, die Anforderungen der DS-GVO und des BDSG an die Datenverarbeitung zu beachten und so beispielsweise Auftragsverarbeitungsverträge mit den Vermietern zu schließen und diese auf die Einhaltung der Informationspflichten nach Art. 13 ff DS-GVO hinzuweisen.

8.3
Versand von automatisiert generierten Eingangsbestätigungen mit personenbezogenen Daten bei Nutzung eines verschlüsselten Kontaktformulars

Stellt ein Dienstleister ein verschlüsseltes Kontaktformular seinen Kunden zur Verfügung, sollte die automatisiert generierte Eingangsbestätigung per E-Mail ohne Mitteilung personenbezogener Daten erfolgen, da nicht sichergestellt werden kann, dass der Anbieter des E-Mail-Dienstes des Kunden eine Transportverschlüsselung ermöglicht.

Ein Bürger machte mich in diesem Jahr auf ein datenschutzrechtliches Problem bei der Verwendung des Kontaktformulars auf der Homepage der Deutschen Bahn aufmerksam. Bei der Nutzung des Kontaktformulars gab der Kunde seine personenbezogenen Daten insbesondere in Form von Kontaktdaten wie Name, Adresse, Telefonnummer etc. an. Diese Informationen wurden über das Kontaktformular verschlüsselt an die Deutsche Bahn übertragen. Anschließend erhielt der Kunde jedoch eine automatisiert generierte Eingangsbestätigung per E-Mail, die alle im Formular angegebenen personenbezogenen Daten beinhaltete.

Der Versand von E-Mails mit personenbezogenen Daten birgt die Gefahr, dass bei einer fehlenden Verschlüsselung Dritte die Kommunikation abgreifen und so Zugang zu den Daten erhalten können. Zwar haben die führenden E-Mail-Dienste-Anbieter in Deutschland bekanntgegeben, eine Transportverschlüsselung bei der Kommunikation untereinander durchgehend einzusetzen („E-Mail made in Germany“), jedoch kann eine vollständige Umsetzung, vor allem bei der Nutzung ausländischer (insbesondere außereuropäischer) Anbieter nicht garantiert werden. Nutzerinnen und Nutzer eines E-Mail-Dienstes sind somit darauf angewiesen, dass Anbieter eine Transportverschlüsselung bei der E-Mail-Kommunikation einsetzen.

Nachdem ich den Konzerndatenschutz der Deutschen Bahn auf dieses Problem hingewiesen habe, wurde eine Änderung im technischen Prozess vorgenommen. Seitdem sind in der automatisiert generierten Rückmail an den Kunden bei Nutzung des Kontaktformulars keine Daten aus dem Kontaktformular mehr enthalten. Dem Kunden wird lediglich eine Eingangsbestätigung mit der Vorgangsnummer per E-Mail zugesandt.

Da mit dieser Anpassung die im Formular durch den Kunden angegebenen Kontaktdaten (Name, Telefonnummer etc.) in der E-Mail nicht mehr übermittelt werden, habe ich die Vorgehensweise für datenschutzrechtlich zulässig erachtet.

9. Gesundheitswesen

9.1 Anforderungen von medizinischen Unterlagen durch gesetzliche Krankenkassen zur Unterstützung der Versicherten bei Behandlungsfehlern

Aufgrund der gesetzlich festgelegten Aufgabenteilung zwischen dem Medizinischen Dienst der Krankenversicherung (MDK) und den Krankenkassen besteht der sozialdatenschutzrechtliche Grundsatz, dass die Krankenkassen grundsätzlich keine medizinischen Daten zur Kenntnis nehmen dürfen. Dies gilt indes nicht bei der Anforderung von Unterlagen durch gesetzliche Krankenkassen zur Unterstützung der Versicherten bei Behandlungsfehlern.

Viele gesetzliche Krankenkassen bieten ihren Mitgliedern an, dass sie sich bei dem Verdacht auf einen Behandlungsfehler an die Krankenkasse wenden können. Dort wird dann Hilfe und ein professionelles Behandlungsfehlermanagement angeboten. Die Krankenkasse prüft den Verdacht auf Behandlungs- oder Pflegefehler sowie Schäden, die durch Medizinprodukte oder Arzneimittel entstanden sein könnten, und unterstützt die Betroffenen bei der Durchsetzung der Ansprüche.

Im Berichtszeitraum erreichten mich hierzu einige Anfragen von Ärzten. Angefragt wurde konkret, ob eine gesetzliche Krankenkasse selbst medizinische Unterlagen zur Unterstützung von Versicherten bei Behandlungsfehlern anfordern darf, ohne den MDK einzuschalten. Letztlich dürfe die Krankenkasse grundsätzlich keine medizinischen Daten zur Kenntnis nehmen.

Rechtliche Bewertung

Im fünften und im zehnten Sozialgesetzbuch (SGB V und SGB X) sind die datenschutzrechtlichen Befugnisse der Krankenkassen umfassend und abschließend geregelt. Entsprechend findet sich dort auch eine Rechtsgrundlage für das geschilderte Tätigwerden der Krankenkasse. Bereits 1989 wurde im SGB V der § 66 eingefügt, der es den Krankenkassen erlaubte, ihre Versicherten bei der Verfolgung von Schadensersatzansprüchen wegen Behandlungsfehlern zu unterstützen.

Auch nach der aktuellen Gesetzesfassung gehört es nach § 66 SGB V zu den Aufgaben der gesetzlichen Krankenkassen, Versicherten bei der Verfolgung von Schadensersatzansprüchen aus Behandlungsfehlern zu helfen, wenn der vermeintliche Behandlungsfehler im Zusammenhang mit der Inanspruchnahme einer Versicherungsleistung der Krankenkasse steht. Die relativ

unbestimmte Vorschrift wurde durch das Gesetz zur Stärkung der Heil- und Hilfsmittelversorgung (Heil- und Hilfsmittelversorgungsgesetz – HHVG) vom 04.04.2017 um die folgenden Sätze 2 und 3 ergänzt:

„Die Unterstützung der Krankenkassen nach Satz 1 kann insbesondere die Prüfung der von den Versicherten vorgelegten Unterlagen auf Vollständigkeit und Plausibilität, mit Einwilligung der Versicherten die Anforderung weiterer Unterlagen bei den Leistungserbringern, die Veranlassung einer sozialmedizinischen Begutachtung durch den Medizinischen Dienst nach § 275 Absatz 3 Nummer 4 sowie eine abschließende Gesamtbewertung aller vorliegenden Unterlagen umfassen. Die auf Grundlage der Einwilligung des Versicherten bei den Leistungserbringern erhobenen Daten dürfen ausschließlich zum Zwecke der Unterstützung des Versicherten bei Behandlungsfehlern verwendet werden."

Diese Erweiterung des § 66 SGB V stellt eine Konkretisierung der in Satz 1 des § 66 SGB V angegebenen Unterstützungsleistung der Krankenkassen dar. Auf dieser Basis kann folglich auch die direkte Herausgabe von Behandlungsunterlagen durch den Arzt an die Krankenkasse erfolgen. Die dazugehörige Vorschrift, die der Krankenkasse erlaubt, zu diesem Zweck entsprechend Daten zu erheben und zu speichern, findet sich in § 284 Absatz 1 Nummer 5 SGB V.

Die Krankenkasse darf die Herausgabe von Patientenunterlagen nach § 66 SGB V an sie selbst jedoch nur fordern, wenn sie sich auf die Unterstützung nach § 66 SGB V, und zwar auf einen näher bezeichneten Behandlungsfall bezieht. Zudem ist Voraussetzung für die Herausgabe, dass eine aktuelle, vom Patienten unterschriebene Erklärung zur Entbindung von der ärztlichen Schweigepflicht mit einer Einwilligung zur Herausgabe an die Krankenkasse vorliegt. Diese Erklärung muss sich auf den konkreten Behandlungsfall beziehen.

Nach § 66 Satz 2 SGB V kann die Krankenkasse auch den MDK mit einer Begutachtung beauftragen. Dementsprechend kann die Krankenkasse die Herausgabe der Behandlungsunterlagen auch an den MDK fordern. Ist dies der Fall, sind die Abschriften der Behandlungsunterlagen gemäß § 276 Abs. 2 Satz 2 SGB V direkt an den MDK zu senden, nicht an die Krankenkasse. Auch der MDK kann gemäß § 276 Abs. 2 Satz 1 SGB V bei entsprechendem Prüfauftrag durch die Krankenkasse selbst Behandlungsunterlagen vom Arzt anfordern.

Im Ergebnis ist festzuhalten, dass es im Rahmen der Unterstützung der Versicherten bei Behandlungsfehlern nach § 66 V SGB mit Einwilligung der Versicherten zulässig ist, dass die Krankenkasse entsprechende Daten ver-

arbeitet. Hierzu dürfen medizinische Unterlagen von den Leistungserbringern auch direkt an die Krankenkasse geschickt werden.

9.2
Glascontainer mit Patientendaten im Krankenhaus

Neben der klassischen Patientenakte gibt es im Krankenhaus auch noch weitere Bereiche, in denen auf den Schutz der Patientendaten geachtet werden muss. Auch bei Entsorgung von „Altglas" kann es zu Datenschutzpannen kommen.

Vor dem 25.05.2018 war in Hessen eine Meldepflicht von Datenschutzvorfällen für Krankenhäuser, die dem HDSIG unterfallen, nicht vorgesehen. Mit dem Wirksamwerden der DS-GVO sind auch die hessischen Krankenhäuser, die im Krankenhausplan stehen, verpflichtet, gemäß Art. 33 DS-GVO selbstständig Datenschutzvorfälle zu melden. Der folgende Fall hat sich in einem hessischen Krankenhaus ereignet:

Der Datenschutzbeauftragte der Klinik wurde von einer Person darauf aufmerksam gemacht, dass ihr auf dem Klinikgelände ein überfüllter Altglascontainer aufgefallen sei. Bei dem Container handelte es sich um einen normalen Standardcontainer, wie er gewöhnlich von den Entsorgungsunternehmen zur Altglassammlung aufgestellt wird. In dem betreffenden Container entsorgte die Klinik Altglas, wie es unter anderem bei Infusionslösungsflaschen oder anderen Flüssigmedikamenten zum Einsatz kommt. Problematisch hierbei war, dass ein nicht unerheblicher Anteil dieser Glasbehälter mit einem zusätzlichen Etikett versehen war. Dieses Etikett enthielt zum Zeitpunkt des Vorfalls einen ausführlichen Datensatz des jeweils betroffenen Patienten mit:

– Patienten-Identifikationsnummer (PID)
– Name, Vorname
– Geburtsdatum
– Adresse
– Krankenversicherungsnummer
– Name der Krankenversicherung
– betroffene Krankenhausstation
– Name des behandelnden Arztes / der behandelnden Ärztin (teilweise)

Durch den offenen Aufbau des Containers war es mühelos möglich, die Daten von einigen Krankenhauspatienten und Krankenhausangestellten einzusehen und einzelne Flaschen zu entwenden.

Getroffene Maßnahmen

Nachdem die Klinik vom Sachverhalt erfahren hatte, hat sie den Vorfall umgehend nach Art. 33 DS-GVO an mich gemeldet.

Um das Risiko der unbefugten Kenntnisnahme durch Dritte zu vermindern, wurden als Sofortmaßnahme die Container in einem abschließbaren Raum untergebracht. Dort sollten sie bis zur Abholung entsprechend unter Verschluss gehalten werden, so dass ausschließlich Mitarbeiter der Klinik und befugtes Personal Zugang haben.

In einem weiteren Schritt hat die Klinik mit dem zuständigen Entsorgungsunternehmen vereinbart, dass die Container auch beim angesetztem Abholtermin nicht mehr öffentlich zugänglich sind.

Anschließend wurde geprüft, welche Daten im Hinblick auf die verwendeten Klebeetiketten für welchen Zweck zwingend erforderlich sind. Zudem wurde gleichzeitig kontrolliert, inwiefern Prozesse derart sinnvoll und verhältnismäßig umstrukturiert werden können, dass an einigen Stellen ggf. keine entsprechenden Daten bzw. Klebeetiketten mehr gebraucht werden.

Dabei stellte sich heraus, dass unter Beachtung des Art. 5 Abs. 1 c DS-GVO an einer signifikanten Zahl von Verwendungsstellen auf einen Großteil der Daten verzichtet werden kann. Die Klinik hat sodann die Vorlagen für die zu verwendenden Klebeetiketten grundlegend überarbeitet und auf die verschiedenen Anwendungsbereiche spezifisch zugeschnittene Klebeetiketten mit entsprechend angepassten Datensätzen entwickelt.

Als weitere Sicherheitsmaßnahmen wurden die Entsorgungsprozesse angepasst, damit eine unbeabsichtigte Kenntnisnahme durch Dritte nicht weiter möglich ist. Dokumente bzw. Formulare, auf denen Etiketten verwendet werden, werden wie bisher datenschutzkonform nach Ablauf der gesetzlichen Aufbewahrungsfristen in die Aktenvernichtung eines zertifizierten Dienstleisters gegeben. Da es für entsprechende Medikamentenverpackungen (insbesondere Glas und Kunststoff) keine zertifizierten Entsorger im Sinne einer datenschutzkonformen Aktenvernichtung gibt und das Entfernen der Etiketten von etwaigen Medikamentenverpackungen kaum oder nur mit unverhältnismäßigen Aufwand möglich ist, wurden die Entsorgungsprozesse für derartige Verpackungen geändert. Diese werden nun an den verarbeitenden Stellen (Stationen der Klinik) gesammelt und täglich in verschlossenen Behältnissen in eine elektromechanische Müllpresse gegeben. Die abgeschlossene Müllpresse befindet sich auf dem Betriebsgelände der Kliniken und kann durch Dritte weder geöffnet noch anderweitig eingesehen werden. Diese Müllpresscontainer werden nach Abholung durch den Entsorger direkt in die abgeschlossene Vorkammer der Müllverbrennungsanlage (sog.

Bunker) entleert, die aus Sicherheitsgründen zutrittsbeschränkt ist. Durch die Entleerung in den Bunker findet im ersten Schritt eine Durchmischung mit anderen Abfällen statt. Im zweiten Schritt wird der Inhalt des Bunkers kontinuierlich durch eine automatische Transportvorrichtung in die Brennkammer weitergeleitet, in der aufgrund der dort herrschenden enormen Temperaturen insbesondere die Etiketten und damit die personenbezogenen Daten unwiederbringlich vernichtet werden.

Fazit

Im vorliegenden Fall hat sich die Klinik meiner Einschätzung nach vorbildlich verhalten und nach Kenntnis des Vorfalles sofort reagiert. In der Folge wurde ein Entsorgungsprozess für die Glasabfälle der Klinik geschaffen, der unter Beachtung von Art. 5 Abs. 1 f DS-GVO das Risiko einer Kenntnisnahme der Patientendaten durch Dritte weitestgehend ausschließt.

9.3
Verlust der Behandlungsdokumentation durch Wasserschäden

Ärztinnen und Ärzte haben geeignete technische und organisatorische Maßnahmen zu treffen, um die Patientendokumentation vor Elementarschäden zu schützen. Der zufällige Untergang der Behandlungsdokumentation stellt eine meldepflichtige Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 33 i. V. m. Art. 4 Nr. 12 DS-GVO dar.

Im Frühjahr und Frühsommer des Jahres 2018 kam es mehrfach zu starken Unwettern in Hessen. Unabhängig voneinander meldeten mir Arztpraxen, dass durch ein Unwetter Wasser in die Keller der Praxen eingedrungen war, in denen Patientenunterlagen aufbewahrt wurden. Hierbei hat das Wasser einen großen Teil der ärztlichen Dokumentation zerstört.

In einem ersten Fall Mitte Mai und damit vor der Geltung der DS-GVO drang das Wasser aus der Kanalisation durch Toilette und Dusche der Praxis in den Keller. Die in der unteren Schublade eines Aktenschrankes lagernden Patientenakten wurden von Kanalisationswasser durchweicht.

Bei einem zweiten Fall Anfang Juni, also nach Geltung der DS-GVO, drückte das Wasser ein Fenster auf und floss durch den darunter stehenden Metallschrank, in dem die Dokumentation aufbewahrt wurde. Alle darin lagernden Karteikarten wurden stark durchnässt. Die Papierdokumente sind in beiden Fällen unlesbar geworden.

Schließlich fand bei einem dritten Fall im Herbst 2018 in einer Arztpraxis durch eine Rohrverstopfung in der Decke des Kellers ein massiver Was-

seraustritt (vermischt mit Fäkalien) statt. Dadurch wurden Patientenakten durchnässt und teilweise stark verschmutzt. Die Akten konnten jedoch auf meinen Hinweis hin getrocknet werden und wurden von der Praxis nach Jahren aufgeteilt, in dichte Säcke verpackt und verschlossen. Nach Aussage der Praxis könnten im Bedarfsfall somit auch die stark verschmutzten Akten jederzeit zur Verfügung gestellt werden.

Rechtliche Bewertung

Fall 1 – Eindringen von Kanalisationswasser in den Kellerraum

Bei der Zerstörung der Dokumentation durch Kanalisationswasser Mitte Mai 2018 im ersten Fall bestand nach dem BDSG-alt noch keine Pflicht für die Praxis, den Verlust der Patientendokumentation zu melden. § 42a BDSG-alt sah eine Mitteilungspflicht an die Aufsichtsbehörden nur vor, wenn die in § 42a Satz 1 BDSG-alt aufgeführten Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.

Mit einem Bußgeld hätte der Vorfall nicht geahndet werden können. Wegen der unzureichenden Sicherung der Unterlagen lag hier möglicherweise zwar ein Verstoß gegen § 9 BDSG-alt vor, da die erforderlichen technischen und organisatorischen Maßnahmen von der Praxis nicht getroffen worden waren. Jedoch war hierfür eine repressive Sanktionierung durch die Mechanismen des Ordnungswidrigkeitenrechts im BDSG a. F. nicht vorgesehen.

Die Praxis führte auf meinen Hinweis eine Kanalsanierung durch und baute eine Rückstausicherung ein, um solchen Schäden vorzubeugen. Dies wies sie mir durch eine Handwerkerrechnung für die durchgeführten Arbeiten nach.

Fall 2 – Eindringen von Wasser durch ein Kellerfenster

Im Fall von Anfang Juni 2018, in dem durch ein Kellerfenster fließendes Wasser die Patientendokumentation unlesbar machte, war hingegen nach neuer Rechtslage ein Verstoß gegen Art. 5 Abs. 1 lit. f DS-GVO anzunehmen. Danach müssen personenbezogene Daten „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')".

Der Verlust der Patientendokumentation stellt eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO dar und ist daher nach Art. 33 DS-GVO in der Regel der Aufsichtsbehörde zu melden, da hier fast immer von einem Risiko für die Freiheiten und Rechte natürlicher Personen

auszugehen ist. Schließlich dient die gesetzliche Dokumentationspflicht auch Zwecken, die primär im Interesse der Patientin bzw. des Patienten bestehen (siehe hierzu etwa Wagner in: MüKo BGB, § 630f Rdnr. 2f., 7. Auflage 2016: „So erleichtert eine gut geführte Patientenakte den Arztwechsel, weil sie dem übernehmenden Mediziner die Anknüpfung an das zuvor Geleistete erleichtert und dadurch die nochmalige Durchführung diagnostischer oder therapeutischer Maßnahmen vermeiden hilft. Weiter gewährleistet die Dokumentation das im Rahmen des allgemeinen Persönlichkeitsrechts anzuerkennende Interesse des Patienten daran, von der eigenen Kranken- und Behandlungsgeschichte Kenntnis nehmen zu können."). Auch die Beweissicherungsfunktion der Dokumentation bzw. ihre Funktion als Beweismittel in einem Arzthaftungsprozess ist vom Gesetzgeber als einer der Regelungszwecke des § 630f BGB anerkannt (BTDrucks. 17/10488 S. 25). Zu diesen Gesetzeszwecken können die bis zur Unlesbarkeit beschädigten Patientenunterlagen nicht mehr verarbeitet werden.

Verstöße gegen die Grundsätze des Art. 5 DS-GVO können nach Art. 83 Abs. 5 DS-GVO mit einem erhöhten Bußgeld geahndet werden. Vorliegend war der Sachverhalt jedoch aufgrund der rechtzeitigen Meldung nach Art. 33 DS-GVO nicht bußgeldrelevant, § 43 Abs. 4 BDSG.

Zukünftig werden die Akten in einen anderen Kellerraum ohne Fenster verbracht, in dem sie weit über dem Boden verwahrt werden. Der Austausch der Fenster, durch die die Wassermassen in den Keller dringen konnten, wurde veranlasst.

Fall 3 – Starke Verschmutzung von Unterlagen durch Rohrbruch

Im letzten Fall aus dem Herbst 2018 war die Dokumentation aufgrund eines Rohrbruchs zwar beschädigt, aber nicht untergegangen. Ein Risiko für die Rechte und Freiheiten natürlicher Personen nach Art. 33 Abs. 1 DS-GVO konnte hier somit verneint werden. Allerdings war vorliegend auch hier eine Meldung nach Art. 33 DS-GVO sinnvoll, da erst auf Hinweis meiner Behörde die Praxis zusagte, sämtliche (auch stark verschmutzte) Unterlagen zu trocknen und bis zum Ablauf der gesetzlichen Aufbewahrungspflicht zu lagern.

Allgemeine Hinweise zur Aufbewahrung von Patientenunterlagen

Die Aufbewahrung von Patientenunterlagen ist nach den in Art. 5 lit. f DS-GVO festgelegten Grundsätzen auszugestalten. Hierzu ist auch ein besonderer Schutz gegen elementare Schäden und Leitungswasserschäden zu treffen. Da Keller besonders überflutungsgefährdet sind, sind bei der Aktenaufbewahrung in Kellern Maßnahmen zu treffen wie z. B.:

– ausreichender Abfluss
– Rückschlagventile (gegen drückendes Wasser aus dem Abfluss)
– dichte Fenster (gegen das drückende Wasser von außen)
– sicherer Standort der Akten (nicht unter einem Fenster, Lagerung ab einer bestimmten Höhe, keine Wasserleitung im Raum)

Zudem sollten die Papierunterlagen und sonstige Datenträger vor Lagerungsschäden im Keller geschützt werden z. B. durch:

– Regulierung der Feuchtigkeit (diese darf nicht zu hoch sein)
– Regulierung der Temperatur (muss gleichbleibend sein)

9.4
Angebot eines „Service-Briefkastens“ durch eine Arztpraxis

Ärztinnen und Ärzte haben geeignete technische und organisatorische Maßnahmen zu treffen, um unbefugten Dritten den Zugang zu Patientendaten zu verwehren. Dies gilt auch dann, wenn sie Rezepte und Überweisungen außerhalb ihrer Praxisräume für ihre Patientinnen und Patienten hinterlegen möchten. Für Unterlagen, die Gesundheitsdaten beinhalten, besteht ein besonderer Schutzbedarf.

Durch eine Eingabe wurde ich darauf aufmerksam, dass eine Ärztin Rezepte und Überweisungen für ihre Patienten zur Abholung in einem öffentlich zugänglichen Briefkasten hinterlegt. Der Schlüssel zum Briefkasten steckte dabei permanent im Briefkasten, so dass berechtigte und nicht berechtigte Personen die dort hinterlegten Unterlagen jederzeit mitnehmen konnten. Auf meine Nachfrage teilte die Ärztin mit, dass die Patientinnen und Patienten meist telefonisch um die Hinterlegung im Briefkasten bäten, um die Unterlagen außerhalb der Öffnungszeiten mitnehmen zu können. Die Rezepte oder Überweisungen würden, in einem verschlossenen Umschlag und mit den Namen der jeweiligen Patientinnen und Patienten beschriftet, in den Briefkasten gelegt. Der Postweg sei hierfür eine unsichere Alternative.

Der Briefkasten befand sich vor dem Eingang zur Praxis, der von der Straße abgeschieden und für Unbeteiligte nicht einsehbar war. Nach Angabe der Ärztin seien bisher keine negativen Rückmeldungen oder missbräuchliche Verwendungen von Inhalten durch Dritte vorgekommen. Gleichwohl schlug sie vor, Aufträge zum Deponieren im Briefkasten zukünftig nur schriftlich einzuholen und ein Zahlenschloss am Briefkasten anzubringen.

Rechtliche Bewertung

Die praktizierte Verfahrensweise war – auch mit den vorgeschlagenen Änderungen – datenschutzrechtlich unzulässig.

Die Aufbewahrung bzw. Hinterlegung von Patientenunterlagen ist nach den in Art. 5 Abs. 1 lit. f DS-GVO festgelegten Grundsätzen auszugestalten.

Trotz eines etwaigen ausdrücklichen schriftlichen Auftrags von Patientinnen und Patienten zur Hinterlegung im Briefkasten bleibt die Ärztin als Inhaberin und Betreiberin des Briefkastens sowie als „Absenderin" der Daten verantwortliche Stelle für die Verarbeitung der Daten im Sinne des Art. 4 Nr. 7 DS-GVO.

Sie trägt weiterhin die Pflichten aus Art. 5 DS-GVO und hat insbesondere durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit personenbezogener Daten zu gewährleisten (Art. 5 Abs. 1 lit. f DS-GVO). Hierzu gehört nach Erwägungsgrund 39 der DS-GVO, dass unbefugte Personen keinen Zugang zu den Daten haben dürfen. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt insbesondere von dem Risiko eines unberechtigten Zugriffs, der Art der Verarbeitung sowie der Bedeutung der Daten für die Rechte und Interessen der betroffenen Person ab. So sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken durch Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten zu berücksichtigen (Art. 32 Abs. 1 und 2 DS-GVO).

Da die Ärztin durch die Übermittlung der Rezepte und Überweisungen Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO verarbeitet, ist Art. 9 Abs. 1 DS-GVO zu beachten. Als besondere Kategorie personenbezogener Daten sind Gesundheitsdaten besonders schützenswert. Aufgrund dessen ist es meiner Auffassung nach unzulässig, die Patienten gänzlich auf den Schutz ihrer Gesundheitsdaten verzichten zu lassen. Eine wirksame Einwilligung scheidet hier schon deswegen aus, weil weder für die Ärztin noch für die Patientinnen und Patienten ersichtlich ist, wer Zugang zu den Daten haben könnte und zu welchen Zwecken diese möglicherweise verwendet werden könnten. Die Patientinnen und Patienten können somit nicht umfänglich informiert in eine solche Übermittlung bzw. Offenlegung einwilligen, die letztlich unübersehbare Gefahren, wie z. B. eine Veröffentlichung im Internet, in sich bergen kann.

Anforderungen an die technisch-organisatorischen Maßnahmen

Im Hinblick auf die Sensibilität der Daten war der durch den permanent vorhandenen Schlüssel stets von jedermann zu öffnende Briefkasten nicht hinnehmbar. Auch die von der Ärztin vorgeschlagene Lösung eines Zahlen-

schlosses mit täglich wechselnden Zugangscodes müsste so ausgestaltet sein, dass die täglich verwendete Zugangsnummer weder für unbeteiligte Dritte noch für Patientinnen und Patienten, die aktuell nichts abzuholen hatten, vorhersehbar ist. So scheidet z. B. die Nutzung der laufenden Tageszahl oder eine feststehende zweistellige Nummer mit laufender Nummer des aktuellen Wochentages als zu leicht überwindbar aus. Es müssten vielmehr zufällige Folgenummern generiert werden.

Ein Standard-Briefkasten ist zudem zum Hinterlegen von Rezepten oder sonstigen ärztlichen Unterlagen mit Patientendaten gänzlich ungeeignet. Weder Material noch Schließsystem stellen einen ernsthaften Widerstand gegen Einbruch oder Vandalismus dar. Ein angemessenes Behältnis für den von der Ärztin angebotenen Service müsste sicherstellen, sein, dass

– das unbefugte Öffnen des Abholbehälters nur mit erheblichem Zeitaufwand und Werkzeugeinsatz möglich ist,
– ein Diebstahl des verschlossenen Behälters durch entsprechende Verankerung weitestgehend verhindert oder erschwert ist und
– eine unbefugte Entnahme durch Dritte über den eventuell vorhandenen Einwurf nicht möglich ist (Sperrklappe oder Blockieren des Einwurfs).

Auch hinsichtlich des Standortes waren erhöhte Anforderungen an den Zugangsschutz zu stellen. Der von der Straße nicht einsehbare Eingangsbereich außerhalb der Praxisöffnungszeiten war insoweit mit hoher Wahrscheinlichkeit weitestgehend unbeobachtet.

Zudem müssten die einzelnen verschlossenen Umschläge mit den bereitgestellten Dokumenten in dem Behältnis deutlich mit den jeweiligen Empfängeranschriften beschriftet sein, damit diese sofort erkennen können, dass das Dokument

– eindeutig aus der Praxis stammt,
– nicht durch Dritte geöffnet wurde,
– der Inhalt vollständig und unverändert ist.

Schließlich stellte sich die Frage, ob überhaupt mehrere Dokumente – und wenn ja, wie viele – pro Tag zur Abholung bereitgestellt werden durften, da nicht ausgeschlossen werden konnte, dass berechtigte Nutzer versehentlich, bös- oder mutwillig fremde Dokumente entfernen oder manipulieren.

Problematisch ist vor allem, dass insbesondere eine missbräuchliche Entnahme immer erst nachträglich auffallen würde: Empfänger, die ihr/e Dokument/e vermissen, könnten frühestens am folgenden Öffnungstag die Praxis kontaktieren. Es ließe sich damit erst im Nachhinein feststellen, ob das angekündigte Dokument nur vergessen oder evtl. durch Dritte entwendet wurde.

Ergebnis

Um den datenschutzrechtlichen Anforderungen bezüglich der Gesundheitsdaten zu entsprechen, hätte die Ärztin eine Schließfach- bzw. Packstation-ähnliche Anlage bereitstellen müssen, die mit den oben beschriebenen Maßnahmen eine geeignete Anzahl von Abholfächern für jeweils einen Patienten (mit zufälligem Wechsel der Zugangsnummer nach jeder Abholung) beinhaltet.

Die von mir aufgestellten technisch-organisatorischen Anforderungen an die Beschaffenheit und den Betrieb eines datenschutzgerechten „Service-Briefkastens“ wollte die Ärztin nicht erfüllen und stellte daher den Betrieb des Briefkastens ein.

9.5
Fortbildungszertifikate der Landesärztekammer Hessen

Fortbildungszertifikate, die zum öffentlichen Aushang in der Arztpraxis oder im Krankenhaus verwendet werden, sollten keine Angaben zum Geburtsdatum und/ oder Geburtsort der Ärztin/des Arztes enthalten. Diese Angaben sind zum Nachweis gegenüber dem Patienten, dass die Ärztin/der Arzt sich entsprechend den berufsrechtlichen Vorgaben fortgebildet hat, nicht erforderlich.

Ein Arzt beschwerte sich darüber, dass auf den von der Landesärztekammer Hessen (LÄKH) ausgestellten Fortbildungszertifikaten außer dem Vor- und Nachnamen sowie der Anrede auch das Geburtsdatum und der Geburtsort abgedruckt werde. Das Fortbildungszertifikat ist ein freiwilliges Angebot der LÄKH an ihre Mitglieder und kann im Mitgliederportal der LÄKH ausgedruckt werden. Obwohl das Zertifikat auch zum Zweck als öffentlicher Aushang in der Arztpraxis oder im Krankenhaus bestimmt ist, war die Angabe und der Ausdruck von Geburtsdatum und Geburtsort vom System zwingend vorgegeben gewesen und ließ sich nicht einschränken.

Auf meine Nachfrage bei der LÄKH zur Erforderlichkeit der Angabe von Geburtsort und Geburtsdatum auf dem Zertifikat erklärte diese, dass ihren Informationen nach Ärztinnen und Ärzte das Fortbildungszertifikat auch zum Nachweis der Erfüllung der Fortbildungspflicht gegenüber der Kassenärztlichen Vereinigung Hessen verwenden würden. Damit dies möglich sei, müsse das Zertifikat eindeutig sein. Das Zertifikat sei so einer bestimmten Person besser zuordenbar. In Abstimmung mit der Anerkennungsstelle der LÄKH wurde die Formulierung des Fortbildungszertifikats durch die LÄKH dennoch dahingehend geändert, dass dieses nunmehr ohne die Angabe des Geburtsortes und des Geburtsdatums erzeugt werden kann.

Aus meiner Sicht müssen Ärztinnen und Ärzte den Patientinnen und Patienten nicht Geburtsdatum und Geburtsort offenlegen, wenn sie den Nachweis führen, dass sie sich entsprechend den berufsrechtlichen Vorgaben fortbilden – schließlich ist der Aushang des Fortbildungszertifikats in der Praxis bzw. im Krankenhaus nicht verpflichtend. Die Missbrauchsgefahr, beispielsweise bei Namensgleichheit, sehe ich bei einem zum Aushang bestimmten Zertifikat eher als gering an. Eine Erforderlichkeit dieser Angaben ist mithin nicht gegeben und vor dem Hintergrund des Grundsatzes der Datensparsamkeit gemäß Art. 5 Abs. 1 lit. c) DS-GVO verzichtbar.

9.6
Prüfung einer Apotheke

In meinen vergangenen Tätigkeitsberichten bildete oft die Prüfung von Arztpraxen und Krankenhäusern einen Schwerpunkt. In diesem Jahr war auch eine Apotheke Gegenstand eines Ortstermins.

Im Februar des Berichtszeitraumes erreichte mich die anonyme Eingabe eines Bürgers: Wie der Eingebende schilderte, seien ihm aus einer öffentlich zugänglichen Papiertonne Schriftstücke „entgegengeflogen“, die personenbezogene Daten enthielten. Diese konnten einer nahegelegenen Apotheke zugeordnet werden. Die aufgefundenen Unterlagen waren der Eingabe beigefügt. Wie sich diesen Unterlagen entnehmen ließ, handelte es sich in erster Linie um Bewerbungsunterlagen und damit um personenbezogene Daten von Beschäftigten i. S. des § 26 Abs. 8 BDSG. Diese waren eigentlich für die Vernichtung vorgesehen.

Ich habe kurzfristig die Apotheke aufgesucht, um den Sachverhalt vor Ort aufzuklären.

Die erwähnten Papiertonnen befanden sich bei meinem Besuch im Hinterhof der Apotheke. Der Hofeingang ist mit einer Tür versehen, die aufgrund der Nutzungsfrequenz meist offensteht, so dass der Hof mit den Papiertonnen nicht nur von außen sichtbar, sondern auch von jedermann zu betreten ist. Der Hinterhof wird zudem auch von den Bewohnern und Besuchern des Hauses genutzt.

Bei meinem nur kurz vorher angekündigten Termin konnte ich in den öffentlich zugänglichen Papiermülltonnen weitere Unterlagen mit personenbezogenen Daten, die sich der Apotheke zuordnen ließen, entdecken (u. a. Rezeptabholscheine und diverse handschriftliche Aufzeichnungen). Die Papiere waren vor der Entsorgung nur grob zerrissen oder zerknüllt worden.

Die „Löschung und Vernichtung“ von personenbezogenen Daten fällt gemäß Art. 4 Nr. 2 DS-GVO unter den Verarbeitungsbegriff der DS-GVO. Nach Art. 5 DS-GVO müssen personenbezogene Daten entsprechend den in Abs. 1 lit. a bis lit. f enthaltenen Grundsätzen verarbeitet werden. Dabei muss die Verarbeitung der personenbezogenen Daten in einer Weise erfolgen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigten Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Wie die Inhaberin der Apotheke einräumte, besaß die Apotheke zwar einen Aktenvernichter, nutzte diesen aber nicht regelmäßig bzw. war sie der Ansicht, dass manche Dokumente nicht so sensibel seien, dass diese fachgerecht vernichtet werden müssten. Außerdem war der Aktenvernichter sowohl von seiner Leistungsfähigkeit als auch von seiner Schutzklasse her angesichts der Sensibilität der zu verarbeitenden Daten ungenügend.

Ich forderte die Inhaberin daher auf, dass sich die Apotheke einen den Anforderungen entsprechenden Aktenvernichter anschafft, mit dem zukünftig sichergestellt ist, dass jeglicher anfallende Papierabfall datenschutzgerecht zerkleinert werden kann.

Gemäß den Anforderungen der DIN 66399 sollte es sich um ein Gerät der Klasse 3, besser der Klasse 4 handeln. Alternativ besteht die Möglichkeit, durch einen zertifizierten Entsorgungsbetrieb eine verschlossene Papiertonne aufstellen zu lassen, bei der die fachgerechte Entsorgung des Inhalts vertraglich und organisatorisch sichergestellt ist.

Anlässlich meiner Ortsbesichtigung stellte ich noch zwei weitere datenschutzrechtlich unzulässige Sachverhalte fest.

Zum Zeitpunkt meines Besuches nutzte die Apotheke eine Wand in unmittelbarer Nähe zum Kundenbereich als Pinnwand für Abholscheine. Mit einem kurzen „Blick um die Ecke“ war es möglich, einzelne Daten, wie zum Beispiel Name oder Medikament, zu erfassen.

Ich habe die Inhaberin der Apotheke aufgefordert, eine alternative Aufbewahrungsmöglichkeit zu finden, um eine ausreichende Datensicherheit und Vertraulichkeit zu gewährleisten.

Des Weiteren wurden im hinteren Arbeitsbereich der Apotheke Bewerbungsunterlagen von abgelehnten Schülerpraktikanten in zwei Stehordnern aufbewahrt. Die abgelehnten Bewerberinnen und Bewerber würden die Unterlagen meist direkt in der Apotheke abholen. Da die Apothekenleitung nicht jeden Tag in ihrem Büro sei, habe man diesen Standort gewählt. Die Ordner trugen

die Aufschrift „Bewerbungen Gut“ sowie „Bewerbungen Schlecht“ und sind für alle Mitarbeiter frei zugänglich. Ich habe auch hier eine organisatorische Abhilfe gefordert.

Ergebnis

Als Ergebnis war festzuhalten, dass die Apotheke noch in einigen Bereichen Nachholbedarf hatte, was einen datenschutzkonformen Apothekenbetrieb anbelangt.

Zwischenzeitlich hat mir die Inhaberin der Apotheke bestätigt, dass ein Aktenvernichter, der meine Anforderungen erfüllt, beschafft wurde. Auch die Mitarbeiter und Mitarbeiterinnen wurden dahingehend sensibilisiert, alle Unterlagen mit personenbezogenen Daten vor der Entsorgung in die Papiertonne nach der vorgegebenen DIN-Norm zu zerkleinern.

Für die Aufbewahrung der Abholscheine wurde ein neues Verfahren eingeführt. Sie sind nun nicht mehr für die Kunden einsehbar.

Auch alle Bewerbungsunterlagen werden ab sofort in einem abschließbaren Büro aufbewahrt und innerhalb der vorgesehenen Frist vernichtet.

Da bei der Datenvernichtung der Grundsatz des Art. 5 Abs. 1 lit. f DS-GVO nicht beachtet wurde, liegt ein Verstoß im Sinne des Art. 83 Abs. 5 lit. a DS-GVO vor. Die unsachgemäße Entsorgung von personenbezogenen Daten kann einen Bußgeldtatbestand erfüllen und wird deshalb nach Abschluss der fachlichen Fallprüfung auch von meiner Bußgeldstelle dahingehend noch geprüft und bewertet werden.

10. Videoüberwachung

10.1
Videoüberwachung im Pflegedienst

In den Geschäftsräumen eines ambulanten Pflegedienstes wurde der Eingangsbereich, der Wartebereich sowie die Anmeldung mittels einer Dome-Kamera permanent überwacht. Nach Prüfung des Sachverhalts wurde die Demontage der Kamera erwirkt.

Die Beschwerdeführerin war Mitarbeiterin in einem ambulanten Pflegedienst. Sie beschwerte sich über die Installation einer Videokamera in den Geschäftsräumen des ambulanten Pflegedienstes. Sie selbst sei als Mitarbeiterin permanent einer Überwachung ausgesetzt. Eine Information durch den Arbeitgeber sei nicht erfolgt, eine Einwilligung durch sie und, soweit ihr bekannt, auch anderer Kolleginnen und Kollegen sei nicht erteilt worden.

Ich habe den Inhaber des Pflegedienstes um Auskunft über die Videoinstallation gebeten. Nach Prüfung der eingegangenen Unterlagen wurde festgestellt, dass eine Dome-Kamera installiert war, die die Eingangstür, den Empfangsbereich sowie den Flur vor dem Eingang überwachte. Als Zweck für die Videoüberwachung wurde angegeben, dass die Kamera zur Vermeidung von Diebstahl sowie Einbruch installiert wurde. Darüber hinaus sollte hierüber erkannt werden, ob ggfs. Seniorinnen und Senioren in Gefahr seien. Eine Speicherung der Daten erfolge nicht.

Die Überwachungseinrichtung war nach Art. 6 Abs. 1, lit. f Datenschutz-Grundverordnung (DS-GVO) zu bewerten.

Gemäß Art. 6 Absatz 1 lit. f. DS-GVO ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Zur Vermeidung eines Diebstahls oder Einbruchs war die Videoinstallation ungeeignet. Ein Nachweis gegenüber Strafverfolgungsbehörden wäre hier nicht möglich gewesen, da keine Aufzeichnung stattfand.

Auch Seniorinnen und Senioren wäre durch die bloße Installation der Überwachung nicht geholfen. Im Falle einer gesundheitlichen Gefahr hätte die Überwachungseinrichtung keine Warnung oder Alarmierung des Rettungsdienstes vorgenommen. Da der Thekenbereich im Foyer dauerhaft besetzt war, erschien die direkte Hilfe durch die Mitarbeiterinnen und Mitarbeiter des

Pflegedienstes betroffener Senioren geeigneter als eine Überwachung der gesundheitsgefährdenden Situation.

Darüber hinaus habe ich bemängelt, dass der Inhaber des Pflegedienstes seinen Informationspflichten gegenüber seinen Mitarbeiterinnen und Mitarbeitern sowie gegenüber Besuchern der Praxisräume nicht umfänglich nachgekommen war. An der Eingangstür zur Pflegedienstpraxis hing zwar ein ca. 8 x 5 cm großer Hinweis auf die Videoüberwachung. Dieser war jedoch nicht im Blickfeld und äußerst dezent am Türblatt in der oberen Ecke angebracht. Sämtliche Informationen zur Videoüberwachung nach Art. 13 ff DS-GVO (u. a. Namen und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zwecke, für die die personenbezogenen Daten verarbeitet werden, Rechtsgrundlage für die Verarbeitung, berechtigte Interessen, die von dem Verantwortlichen verfolgt werden) fehlten. Auch weitere Informationen, schriftlich – z. B. per Rundschreiben – oder mündlich – z. B. in einer internen Dienstbesprechung – erfolgten nicht.

Ich habe deshalb eine Anhörung gemäß § 28 HVwVfG durchgeführt, da ich beabsichtigte, eine Beseitigungsanordnung gemäß Art. 58 Absatz 2 lit. f DS-GVO gegenüber dem Inhaber des ambulanten Pflegedienstes zu erlassen.

Die Anweisung, die Videoüberwachung zu beseitigen, konnte jedoch unterbleiben, da mir die ersatzlose Demontage der Videokamera vor Ablauf der Frist zur Stellungnahme nachgewiesen wurde.

10.2
Einsatz von Videoüberwachung zur Vermeidung von „wildem Müll“

Die Installation einer Videokamera ist in der Regel nicht statthaft, um die Verursacher von sogenanntem wildem Müll zu überführen.

Obwohl in Hessen eine Abfallwirtschaft betrieben wird, die es den Bürgern erlaubt, ihren Müll in den meisten Fällen kostenfrei zu entsorgen, ist die unzulässige Ablagerung von Müll an Straßen, Glascontainern, Waldparkplätzen, auf Feldwegen und vielen andern Stellen ein großes Problem. Bleibt der Müll zu lange liegen, werden oft anderer Müll oder gar schadstoffhaltige Abfälle von anderen Bürgern dazugestellt.

Diese Art der Müllentsorgung wird als Ordnungswidrigkeit oder als Straftat behandelt und ist bußgeldbewehrt. Dies scheint jedoch nicht effektiv abzuschrecken.

a) Problematik an öffentlichen Plätzen

Für die Beseitigung des Mülls an öffentlichen Plätzen ist der Verursacher verantwortlich. Ist dieser nicht zu ermitteln, haftet der Grundstückseigentümer für die Entsorgung. In den meisten Fällen sind das die Kommunen. Der Abfall ist nicht nur eine große Umweltbelastung, er bindet auch Personal und Kosten, die in der Folge auf die Allgemeinheit umgelegt werden.

Um der wilden Müllplätze Herr zu werden und einer Bildung von Schmutzecken vorzubeugen, kamen im Berichtszeitraum mehrere Kommunen auf die Idee, eine Videoüberwachung in bestimmten innergemeindlichen Bereichen zu installieren, und fragten mich, unter welchen Voraussetzungen dies in die Tat umgesetzt werden könne.

Das Anliegen der Kommunen mag nachvollziehbar sein. Es bestand jedoch für die Vorhaben jeweils keine Rechtsgrundlage, die dieses Vorgehen zulassen würde.

Im Rahmen der Gefahrenabwehr dürfen die Ordnungsbehörden Videoüberwachungsmaßnahmen an Orten durchführen, an denen schon verschiedentlich Straftaten begangen wurden und die Gefahr besteht, dass weitere Straftaten begangen werden. Eine derartige Überwachung hat zudem stets offen zu erfolgen (§ 14 Abs. 4 HSOG).

Beide Voraussetzungen waren in den vorgetragenen Fällen nicht gegeben. Es handelte sich nicht um Kriminalitätsschwerpunkte i. S. d. HSOG und die Überwachungen sollten jeweils verdeckt erfolgen. Die geplanten Maßnahmen waren unverhältnismäßig. Neben einer Videoüberwachung gab es weitere geeignete Möglichkeiten, um Ablagerungen zu verhindern. Die Überwachung von öffentlichen Plätzen sollte immer Ultima Ratio, also das letzte Mittel der Wahl sein, andere Lösungswege sind grundsätzlich zu bevorzugen. So könnte beispielsweise der öffentliche Raum so gestaltet werden, dass durch bauliche Maßnahmen oder durch einen geregelten Zugang die Ablagerung von wildem Müll verhindert wird.

Bei einer weiteren Anfrage handelte es sich um die beabsichtigte Überwachung eines Waldparkplatzes. Hier war öffentlich zugänglicher Raum betroffen, der von jedermann betreten werden kann (§ 15 Abs. 1 HWaldG). Abzuwägen war daher, ob Anhaltspunkte dafür bestanden, dass schutzwürdige Interessen der von der Videoüberwachung betroffenen Personen überwogen. In Abwägung der Interessen wirkten die Persönlichkeitsrechte der Waldbesucher schwerer. Auch bei der Prüfung, ob es sich um eine Videoüberwachung nach den Gesichtspunkten zur Strafverfolgung nach dem Ordnungswidrigkeitsgesetz in Verbindung mit der Strafprozessordnung handelte, kam ich zu keinem anderen Ergebnis. Die Zulässigkeit einer Videoüberwachung war auch hier

zu verneinen. Bei einer Videoüberwachung würden nicht nur die Personen gefilmt werden, bei denen es zu einem Fehlverhalten käme, sondern lückenlos alle Besucher des öffentlichen Parkplatzes. Dieser Umstand greift zu weitreichend in die Persönlichkeitsrechte der Waldbesucher ein.

Denn grundsätzlich bleibt zu berücksichtigen, dass der Effekt einer Videoüberwachung zur Vermeidung von wildem Müll an öffentlichen Plätzen schnell ins Leere läuft. Sobald die Kamera entdeckt wird – und das wird sie zwangsläufig sehr schnell aufgrund der bestehenden Transparenzpflichten, die die Datenschutzgrundverordnung erfordert – erfolgt die Müllablagerung an der nächsten sich bietenden Gelegenheit.

b) Problematik in Wohnanlagen

Insbesondere von Bewohnerinnen und Bewohnern bzw. Wohnungsbaugesellschaften dicht besiedelter Stadtgebiete und Wohnhochhäusern erreichten mich sowohl Beschwerden zu bestehenden Videoüberwachungen der Müllplätze als auch Anfragen zur Neuerrichtung von Überwachungsanlagen.

Bei einem Wohnhochhaus kam ich zu dem Ergebnis, dass die Wohnungsbaugesellschaft als Betreiberin der Kamera diese weiterhin einsetzen darf. Es konnte detailliert vorgetragen und belegt werden, wann und wie oft es zu groben Verstößen kam, die zu hohen Kosten der Eigentümergemeinschaft führten. Das berechtigte Interesse i. S. v. Art. 6 Abs. 1, lit. f DS-GVO konnte ich bejahen.

In einem anderen Fall war die Kamera abzubauen. Die Kamera war von der Hauswand eines Mehrfamilienhauses auf den Müllplatz auf der gegenüberliegenden Straßenseite gerichtet. Art und Häufigkeit der Verunreinigungen wurden nicht vorgetragen. Die Interessen und die mit der Überwachung einhergehende Persönlichkeitsverletzung der Passanten und Mieter wurden als schwerwiegender erachtet als die nicht hinreichend erklärten Interessen des Betreibers.

10.3
Private Videoüberwachung des öffentlichen Raumes

Zahlreiche Beschwerden erreichten mich wieder von Passanten und Anwohnern, die von privaten Grundstücken auf den öffentlichen Bereich ausgerichtete Videoüberwachungsanlagen betrafen. Ebenso gaben Ordnungsbehörden etliche bei ihnen angezeigte Vorkommnisse zum selben Thema zuständigerweise an mich ab.

Eine Videoüberwachung Privater von öffentlichen Straßen, Gehwegen und Plätzen ist in der Regel unzulässig. Das habe ich bereits in früheren Tätigkeitsberichten thematisiert (siehe u. a. 46. TB, Ziff. 11.4; 45. TB, Ziff. 5.2.1, 43. TB, Ziff. 5.2.1.2). Unter Geltung der Datenschutz-Grundverordnung (DS-GVO) hat sich hieran nichts geändert. Dies zeigen folgende Beispiele.

Ein Kamerabetreiber hatte seine Kamera auf den Gehweg und die Straße vor seinem Grundstück ausgerichtet, um sein dort häufig abgestelltes Fahrzeug zu überwachen. Zur Rechtfertigung reichte er eine Strafanzeige wegen Sachbeschädigung des Fahrzeuges ein. Eine Rechtfertigung für die Videoüberwachung des öffentlichen Raums war das nicht. Abgesehen davon, dass eine Überwachung auch durchgeführt wurde, wenn das Fahrzeug dort nicht angestellt war, ist das Parken von Kraftfahrzeugen keine Form des Anliegergebrauchs. Die Videoüberwachung war nach den Maßstäben des Art. 6 Abs. 1, lit. f) DS-GVO zu werten.

Die Begründung einer einmaligen Sachbeschädigung des Kraftfahrzeugs habe ich, angesichts einer dauerhaften Überwachung des öffentlichen Raumes vor dem Grundstück rund um die Uhr, als nicht ausreichend erachtet. Die Kamera war abzubauen.

In einem anderen Fall hatte ein selbstständiger Handwerker zwei Kameras von seiner Hauswand in den öffentlichen Bereich gerichtet. Vorfälle wurden durch den Kamerabetreiber nicht beschrieben. Als Begründung wurde vorgebracht, dass vor der Grundstücksgrenze im öffentlichen Raum das Handwerkerfahrzeug geparkt wurde, das Werkzeuge beinhalte. Die Überwachung erfolge rein vorsorglich.

Als Zweck wurden Hausrecht sowie Vandalismusprävention angegeben. Ein Hausrecht im öffentlichen Raum (etwa ein Hausrecht am Pkw) besteht aber nicht. Eine Überwachung des öffentlichen Raums ist auch zu präventiven Zwecken unzulässig. Auch diese Kameras waren abzubauen.

Da es immer wieder zu Nachfragen und fehlerhaften Einschätzungen bei der Errichtung und beim Betrieb einer Überwachungskamera kommt, hier noch einmal zusammenfassend, was erlaubt ist und was nicht:

1. Die Kamera darf nur das eigene Grundstück filmen. Auf schwenkbare Kameras sollte verzichtet werden.
2. Aufnahmen öffentlicher Bereiche, wie Straßen und Gehwege, sind in der Regel verboten.
3. Wer unrechtmäßig gefilmt wird, kann Unterlassung und Schadenersatz verlangen.

4. Besucher sollten auf die Überwachung aufmerksam gemacht werden.
5. Das Nachbargrundstück darf nicht gefilmt werden.

10.4
Videoüberwachung in der Gastronomie

Wo sich Menschen zur Freizeitgestaltung bzw. zum Verzehr von Speisen und Getränken aufhalten, darf während der Öffnungszeiten in der Regel keine Videoüberwachung stattfinden.

Im Berichtsjahr sind bei mir vermehrt Beschwerden über Videoüberwachung in Gastronomiebetrieben (sowohl Innen- als auch Außengastronomie) eingegangen. Betroffen waren Döner-Läden, Eisdielen, Schwimmbadgastronomie sowie eine Reihe von Speisegaststätten. In mehreren Fällen habe ich die Beseitigung der Kameras erfolgreich angeordnet. Die Kameras wurden abgebaut.

Der Arbeitskreis Wirtschaft der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (ehemalige Bezeichnung: Düsseldorfer Kreis) führte bereits in seiner Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ vom 19.02.2014 unter Ziff. 3.2 den gemeinsamen Standpunkt der Aufsichtsbehörden zur Überwachung in Gastronomiebetrieben aus:

> „Die Videoüberwachung des Gastraumes einer Gaststätte ist nach § 6b BDSG (a. F.) im Regelfall datenschutzrechtlich unzulässig. Jedenfalls die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind Kundenbereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und damit nicht mit Videokameras überwacht werden dürfen.
>
> Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechtigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann.“

Daran hat sich durch die neue Rechtslage nichts geändert, maßgeblich ist jetzt Art. 6 Abs. 1, lit. f) DS-GVO. Betreiber von Gastronomiebetrieben sollten daher entsprechende Vorhaben streng an der Orientierungshilfe messen. In der Regel ist eine Videoüberwachung datenschutzrechtlich unzulässig. Fundstelle der Orientierungshilfe: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/OH_Videoueberwachung%20nicht%20oeffentliche%20Stellen.pdf

10.5
Videoüberwachung in Schwimmbädern

Die Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna ist unzulässig.

Auch in diesem Jahr erreichten mich mehrere Beschwerden hinsichtlich der Videoüberwachung in Schwimmbädern. Eine Beschwerde richtete sich gegen die Überwachung im Sammelumkleidebereich eines mittelhessischen Schwimmbads.

Die Überwachungseinrichtung war nach Art. 6 Abs. 1, lit. f DS-GVO zu bewerten.

Gemäß Art. 6 Absatz 1 lit. f. Datenschutzgrundverordnung (DS-GVO) ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Ich stellte fest, dass der Betreiber insgesamt zwölf Kameras und zwei Kameraattrappen im Schwimmbad installiert hatte. Nach Prüfung und Auswertung wurde die Videoüberwachung wie folgt vor Ort datenschutzkonform hergestellt:

– Im Eingangsbereich an den Drehkreuzen zur Schwimmhalle und zur Sauna, sowie an der Kasse und am Kassenautomat (eine Überwachung von Beschäftigten fand nicht statt) wurde die Aufzeichnung während der Öffnungszeiten eingestellt und auf die Zeiten außerhalb der Öffnungszeiten reduziert. Zu den Öffnungszeiten war Personal vor Ort, so dass eine Überwachung zu diesen Zeiten nicht notwendig war.
– Die Kameras am Eingang und Ausgang der Rutschen blieben zur Unterstützung des Aufsichtspersonals installiert. Die Aufzeichnungsfunktion wurde deaktiviert.
– Die Speicherdauer der verbliebenen aufzeichnenden Kameras wurde auf 72 Stunden reduziert.
– Kameras im Umkleidebereich, am Drehkreuz zum Fitness-Studio sowie eine Kameraattrappe im Familienumkleidebereich wurden entfernt.
– Die Hinweisbeschilderungen wurden gemäß der Datenschutzgrundverordnung angepasst und erweitert.

In Ergänzung verweise ich auf meine Ausführungen zur Videoüberwachung in Schwimmbädern im 44. Tätigkeitsbericht 2015, Ziff. 8.2. Die dort vorgestellte Orientierungshilfe zur Videoüberwachung in Schwimmbädern wurde überarbeitet und mit Stand vom 08.01.2019 veröffentlicht (siehe auch Anhang I 3.2).

11. Wirtschaft, Banken, Selbstständige

11.1
Übermittlung von Daten durch Banken an geschiedene Ehepartner

Die Übermittlung personenbezogener Daten durch Banken und Sparkassen an Ehepartner ist nur dann zulässig, wenn diese aufgrund einer Vollmacht oder Kontoinhaberschaft zum Empfang der Daten berechtigt sind. Auf die Ehe allein kann eine Übermittlung hingegen nicht gestützt werden.

Im Berichtsjahr sind mir einige Beschwerden vorgelegt worden, welche die Übermittlung personenbezogener Daten an bereits geschiedene Ehepartner durch Banken und Sparkassen zum Gegenstand hatten. In sämtlichen mir zur Kenntnis gebrachten Vorgängen war die Datenübermittlung unzulässig.

Es handelte sich um zwei Fallkonstellationen:

a. die Herausgabe einer aktuellen Kontenübersicht, auf der auch die Konten und Kontostände des geschiedenen Ehepartners aufgeführt waren und
b. die Zusendung von Zweitschriften von Kontoauszügen zum Girokonto an den geschiedenen Ehepartner.

Bei Fallkonstellation a) beantragte jeweils eine Einzelperson eine Übersicht seiner/ ihrer Konten, die aufgrund der bekannten und in der Datenverarbeitung auch gespeicherten Ehe auch ausgehändigt wurde. Darin waren auch alle Konten des geschiedenen Ehepartners, für die weder eine Vollmacht noch eine Mitkontoinhaberschaft bestand, enthalten. Bei Fallkonstellation b) beantragte eine Person Zweitschriften von Kontoauszügen zu dem eigenen Konto, die dann an die Postanschrift des geschiedenen Ehepartners gesandt wurden.

Beide Fallbeispiele stellten unzulässige Übermittlungen personenbezogener Daten dar, weil der Ehepartner nicht Kontoinhaber war und auch keine Kontovollmacht vorlag.

Grundsätzlich ist eine Datenübermittlung nur dann zulässig, wenn diese auf die Regelungen des Art. 6 Abs. 1 DS-GVO gestützt werden kann.

Art. 6 DS-GVO

(1) [1]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.

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

Vorliegend erfüllte keine der beiden Fallkonstellationen die Voraussetzungen des Art. 6 Abs. 1 DS-GVO.

Sind beide Ehepartner gemeinsam Vertragspartner bei der Bank, z. B. im Rahmen einer gemeinsamen Immobilienfinanzierung, dürfen die Daten zu diesem Vertrag nach Art. 6 Abs. 1 lit. b) DS-GVO selbstverständlich auch an den geschiedenen Ehepartner übermittelt werden. Gleiches gilt, wenn der Empfänger eine auch nach der Scheidung wirksame Vollmacht für das Konto hat, zu dem Daten übermittelt werden. Die Ehe allein stellt hingegen keinen Erlaubnistatbestand dar. Daher wirkt sich eine Scheidung in der Regel auch nicht auf die Zulässigkeit der Datenübermittlung zu dem betroffenen Vertragsverhältnis aus.

Die Ursache für die fehlerhafte Übermittlung in den mir als Beschwerde vorgebrachten Sachverhalten lag in allen Fällen in der Speicherung und unzureichenden Korrektur von Personenverbünden und deren fehlerhafte Beurteilung durch die Bank.

Banken erstellen bei Eheleuten in ihrer Bankanwendung aus verschiedenen Gründen sogenannte Personenverbünde (hier u. a. Eheleute). Dies ist z. B. im Rahmen der Erteilung von Freistellungsaufträgen von Bedeutung oder auch, um eine Übersicht über das Gesamtengagement der Eheleute zu haben. Diese Personenverbünde beinhalten auch die jeweiligen Postanschriften der Ehepartner. Innerhalb der Personenverbünde bestehen häufig gegenseitige Kontovollmachten oder gemeinsame Kontoinhaberschaften, die zum gegenseitigen Empfang von personenbezogenen Daten berechtigen.

In Fallkonstellation b) wurden die Zweitschriften von Kontoauszügen aufgrund der zum Personenverbund gespeicherten Postanschriften an die Postanschrift des bereits geschiedenen Ehepartners gesendet. Dieser war jedoch zum Empfang der Daten nicht berechtigt.

Eine Empfangsberechtigung besteht innerhalb von Personenverbünde nicht ausnahmslos. Daher ist auch bei bestehenden Personenverbünden die jeweilige Berechtigung zum Erhalt personenbezogener Daten im Einzelfall zu prüfen und zu beachten.

Dies war in den hier zu behandelnden Fällen nicht ausreichend erfolgt. Zusätzlich gelangten die Daten an einen bereits geschiedenen Ehepartner, was von den betroffenen Personen als besonders kritisch empfunden wurde. In laufenden Scheidungsverfahren kann sich die unzulässige Übermittlung von personenbezogenen Daten auch auf die laufenden Verhandlungen oder das gerichtliche Verfahren auswirken.

Kreditinstituten wird daher zur Vermeidung derartiger Fehler empfohlen, anstelle der gespeicherten Personenverbünde die jeweilige Empfangsberechtigung zu prüfen und gespeicherte Personenverbünde bei Scheidungsverfahren zu korrigieren bzw. den Eheleuteverbund zu löschen.

Ich habe daher in allen Fällen die Banken dazu aufgefordert, die entsprechende Löschung der Personenverbünde sowie die Anpassung der hinterlegten Anschriften vorzunehmen.

11.2
Datenpanne bei Mastercard und Mastercard Priceless Specials

Die Datenpanne bei Mastercard Europe SA (Mastercard), von der nach dem Ergebnis der bisherigen Untersuchungen nur das Kundenbindungsprogramm Mastercard Priceless Specials Germany betroffen war, hat gezeigt, wie leicht das Vertrauen in den Datenschutz und die Datensicherheit erschüttert werden kann und welche Aufwände durch einen solchen Vorfall bei der verantwortlichen Stelle und den Aufsichtsbehörden bereits durch die Bearbeitung von Anfragen und Beschwerden entstehen. Schon deshalb sollten verantwortliche Stellen penibel darauf achten, dass keine Sicherheitslücken entstehen.

Mastercard wurde am 19.08.2019 durch Dritte darauf aufmerksam gemacht, dass eine Liste mit Kunden von Mastercard, die etwa 90.000 Personen umfasst hat, im Internet veröffentlicht wurde. In dieser Liste war neben den Namen der betroffenen Personen auch deren Geburtsdatum, die Postanschrift, die E-Mail-Adresse und die vollständige Kreditkartennummer enthalten. Das

Ablaufdatum von Kreditkarten und die Prüfziffer (CVC) waren von dem Datenschutzvorfall nicht betroffen.

Der Datenschutzvorfall hat innerhalb kürzester Zeit zu einer hohen Zahl von Beschwerden an meine Behörde geführt. Häufige Beschwerdegegenstände waren eine fehlende Entschuldigung für den Vorfall durch Mastercard, Bedenken hinsichtlich des Erhalts von größeren Mengen Spam-Mail und eine allgemeine Verunsicherung aufgrund der Veröffentlichung persönlicher Daten. Der Inhalt der Beschwerden hat deutlich gezeigt, dass bereits die Veröffentlichung von üblicherweise nicht jedermann zugänglicher Daten, wie das Geburtsdatum, E-Mail-Adresse und Kreditkartennummer, bei den betroffenen Personen zu einer starken Betroffenheit führen kann. Besonders deutlich zu spüren war ein starker Vertrauensverlust in das Kreditkartenunternehmen Mastercard, das als Bestandteil der Kreditwirtschaft im Allgemeinen einen hohen Vertrauensvorschuss beim Datenschutz und der vertraulichen Behandlung von Kundendaten genießt. Diese Verunsicherung bestand, obwohl betroffene Personen einen materiellen Schaden nicht darstellen konnten und mir Missbrauchsfälle bislang nicht zur Kenntnis gelangt sind.

Mastercard war aufgrund des Vorfalls zur Meldung dieser Datenschutzverletzungen an die zuständige Aufsichtsbehörde gemäß Art. 33 DS-GVO verpflichtet, sobald Mastercard diese festgestellt hatte. Eine solche Meldung wurde bei mir eingereicht, obwohl zu diesem Zeitpunkt noch unklar war, welche Aufsichtsbehörde in Europa für die Datenschutzverletzung zuständig ist. Die weltweite Marktpräsenz von Mastercard erforderte zunächst, die für den Datenschutzvorfall zuständige Aufsichtsbehörde innerhalb der Europäischen Union festzustellen.

Die weitaus meisten Personen, die von dem Vorfall betroffen waren, haben ihren Wohnsitz in Deutschland. Auch richtet sich das Kundenbindungsprogramm Mastercard Priceless Specials Germany nur an Kunden mit einem Wohnsitz in Deutschland. Allerdings waren auch Personen von dem Vorfall betroffen, die ihren Wohnsitz außerhalb Deutschlands haben. Mastercard ist in der gesamten Europäischen Union tätig und unterhält in Deutschland ein Repräsentanzbüro in Eschborn bei Frankfurt am Main. Bei diesem Repräsentanzbüro handelt es sich entsprechend Erwägungsgrund 22 DS-GVO um eine Niederlassung im Sinne der DS-GVO. Die Hauptniederlassung von Mastercard für die Europäische Union hat ihren Sitz jedoch in Belgien. Die Daten wurden außerdem durch einen Auftragsverarbeiter in Österreich verarbeitet. Folglich bestand eine grenzüberschreitende Datenverarbeitung im Sinne von Art. 4 Nr. 23 lit. b) DS-GVO.

Für die Behandlung der grenzüberschreitenden Datenverarbeitung hat die DS-GVO hinreichend Vorsorge getroffen. Auch bei einer grenzüberschrei-

tenden Datenverarbeitung bleibt zunächst jede Aufsichtsbehörde gemäß Art. 56 Abs. 2 DS-GVO für die Entgegennahme von Beschwerden zuständig. Erkennt diese jedoch, dass eine grenzüberschreitende Datenverarbeitung vorliegen kann, informiert sie die für die Hauptniederlassung oder einzige Niederlassung in der Europäischen Union zuständige und damit federführende Behörde unverzüglich über die Angelegenheit. Die Aufsichtsbehörden stimmen dann die weitere Bearbeitung untereinander ab. Entscheidet die federführende Behörde, das Verfahren an sich zu ziehen, übernimmt diese die Federführung im Sinne von Art. 60 DS-GVO und koordiniert das weitere Vorgehen. Dies war hier der Fall.

Aufgrund der grenzüberschreitenden Datenverarbeitung habe ich Kontakt zur Datenschutzbehörde des Mitgliedstaates Belgien aufgenommen. Die Datenschutzbehörde des Mitgliedstaates Belgien hat nach kurzer Prüfung aufgrund ihrer Zuständigkeit für die Hauptniederlassung von Mastercard in der Europäischen Union gemäß Art. 56 Abs. 4 DS-GVO entschieden, sich mit dem Vorgang als federführende Aufsichtsbehörde zu befassen. Damit übernahm die Datenschutzbehörde des Mitgliedstaates Belgien gemäß Art. 56 Abs. 1 DS-GVO die Koordinierung für die Bearbeitung der aufsichtsrechtlichen Aufgaben.

Die DS-GVO sieht in diesem Fall vor, dass die federführende Aufsichtsbehörde gemäß Art. 60 DS-GVO mit anderen Aufsichtsbehörden, die von dem Vorgang ebenfalls betroffen sind, zusammenarbeitet. Hierbei versucht die federführende Aufsichtsbehörde, zwischen allen betroffenen Aufsichtsbehörden einen Konsens zu erzielen, und erarbeitet, sofern dies erforderlich ist, einen Beschlussentwurf. Sind alle betroffenen Aufsichtsbehörden mit dem Beschlussentwurf einverstanden, wird dieser von der federführenden Aufsichtsbehörde erlassen und der Hauptniederlassung oder einzigen Niederlassung des Verantwortlichen mitgeteilt.

In Ausführung dieser Regelungen hat sodann die Datenschutzbehörde des Mitgliedstaates Belgien in Abstimmung mit mir die Aufklärung des Sachverhalts und die Untersuchung der Gründe für den Datenschutzverstoß übernommen. In Abstimmung mit der Datenschutzbehörde habe ich aufgrund meiner Zuständigkeit für das Repräsentanzbüro von Mastercard alle Tätigkeiten der Aufsichtsbehörden in Deutschland koordiniert. Dies beinhaltet auch die Bearbeitung der bei mir eingehenden Beschwerden und deren Beantwortung.

Aufgrund des von wenigen Ausnahmen abgesehen weitgehend gleichen Beschwerdeinhalts aller Beschwerden wurden diese von mir einheitlich beantwortet. Sofern andere Aufsichtsbehörden in Deutschland dies gewünscht hatten, habe ich diesen ebenfalls ein Schreiben zur Beantwortung der bei ihnen eingereichten Beschwerden zur Verfügung gestellt. Zur aktuellen

Information wurden außerdem alle betroffenen Personen über eine Webseite im Internet unter der Adresse https://datenschutz.hessen.de/datenpanne-bei-mastercard-priceless-specials-deutschland über den weiteren Vorgang der Angelegenheit unterrichtet. Alle betroffenen Personen können sich dort jeweils aktuell informieren.

Aus der Aufklärung des Sachverhaltes ergab sich, dass Mastercard dafür Sorge getragen hat, dass die im Internet verfügbaren personenbezogenen Daten unverzüglich gelöscht wurden. Dennoch konnten die Daten bereits vor der Löschung von Dritten kopiert werden. Durch die vorgenommenen Löschungen konnte daher nicht sichergestellt werden, dass die veröffentlichten Daten nicht mehr genutzt oder weiterverbreitet werden. Mastercard überwacht daher das Internet auf weitere Veröffentlichungen der Daten und hat deren Löschung veranlasst oder wird deren Löschung veranlassen.

Auch die betroffenen Personen wurden von Mastercard über den Vorfall informiert. Mastercard hat außerdem unter https://www.mastercard.de/de-de/faq-pricelessspecials.html eine FAQ-Liste mit weiteren Details zu der Datenpanne veröffentlicht, mit deren Hilfe sich betroffene Personen über die von Mastercard empfohlenen Maßnahmen und den aktuellen Stand der Untersuchungen informieren können. Betroffene Personen können sich unter der Emailadresse Germany@mastercard.com auch direkt an Mastercard wenden, um weitere Informationen zu erhalten. Als eines der Hauptrisiken wurde in der Zusammenarbeit mit Mastercard die Möglichkeit von Phishingattacken auf betroffene Personen erkannt. Darüber wurden die betroffenen Personen informiert und diese wurden um erhöhte Wachsamkeit gebeten.

Die weitere Untersuchung des Vorgangs durch einen von Mastercard beauftragten und auf derartige Vorgänge spezialisierten Dienstleister ergab, dass die Datenpanne wie zu Beginn der Untersuchungen angenommen auf das Programm Mastercard Priceless Specials Germany beschränkt und das Zahlungsverkehrsnetz von Mastercard nicht betroffen war.

Aufgrund des bisher bekannten Sachverhalts bestehen daran auch keine Zweifel. Der mit dem Betrieb von Mastercard Priceless Specials Germany beauftragte Dienstleister hat keinen Auftrag zum Betrieb oder Durchführung weiterer Programme von Mastercard. Der Dienstleister ist insbesondere nicht in den Betrieb des Zahlungssystems von Mastercard eingebunden.

Eine weitere Untersuchung von Details zu dem Vorfall ergab, dass vor allem Sicherheitsprobleme bei dem von Mastercard beauftragten Dienstleister zu dem Datenschutzverstoß geführt haben. Es deutet vieles darauf hin, dass ein Missbrauch von Zugangsrechten zu dem Vorfall beigetragen hat. Die Untersuchung hat mehrere Wochen in Anspruch genommen, was von mir

nicht bemängelt wurde. Die von Mastercard veranlassten Maßnahmen halte ich für ausreichend.

Für betroffene Personen besteht grundsätzlich gegenüber Mastercard oder gegenüber einem von Mastercard mit der Datenverarbeitung beauftragten Unternehmen gemäß Art. 82 DS-GVO ein Schadensersatzanspruch. Ein Schaden kann z. B. durch den vorsorglichen Umtausch der Kreditkarte oder damit im Zusammenhang stehender Aufwände entstehen. Die beteiligten Kreditinstitute wurden von Mastercard allerdings bereits darüber unterrichtet, dass Mastercard Aufwände im Zusammenhang mit dem Umtausch von Kreditkarten ersetzt und die Aufwände von den beteiligten Kreditinstituten gegenüber betroffenen Kreditkarteninhabern nicht geltend gemacht werden sollen. Schäden durch den Umtausch von Kreditkarten sollten betroffenen Personen daher in der Regel nicht entstehen. Sollten dennoch Schäden entstanden sein, können Schadensersatzansprüche direkt gegenüber Mastercard beziffert und geltend gemacht werden. Die Datenschutzaufsichtsbehörden können dabei allerdings nicht unterstützen.

Neben Schadensersatzansprüchen bestehen Ansprüche von betroffenen Personen gemäß Art. 15 ff. DS-GVO. In Betracht kommen insbesondere Ansprüche auf Auskunft nach Art. 15 DS-GVO und auf Löschung nach Art. 17 DS-GVO.

Zur Erteilung von Auskünften nach Art. 15 DS-GVO hat Mastercard ein Portal eingerichtet. Dies wird von mir nicht bemängelt. Das Portal wird von Mastercard betrieben und zur Erteilung von Auskünften werden nur die Daten abgefragt, die zur Auskunftserteilung und zur Identifikation der anfragenden Personen erforderlich sind. Die Identifikation ist notwendig zur Vermeidung einer Auskunftserteilung an unbefugte Personen und dient daher vor allem dem Schutz betroffener Personen. Da von der Veröffentlichung auch die von den betroffenen Personen genutzten E-Mail-Adressen betroffen waren, bittet Mastercard aus Sicherheitsgründen um Nutzung des eingerichteten Portals. Auch das wird von mir nicht bemängelt. Dennoch habe ich Mastercard darauf hingewiesen, dass auch ohne Nutzung des Portals eingegangene Anfragen auf Selbstauskunft gemäß Art. 15 DS-GVO zu bearbeiten sind und den betroffenen Personen Auskunft zu erteilen ist.

Ein gesetzlicher Löschungsanspruch nach Art. 17 DS-GVO besteht jedoch nicht. Mastercard ist zur Dokumentation der bisherigen Teilnahme von betroffenen Personen an dem Programm handelsrechtlich verpflichtet und berechtigt. Vorhandene Zugangskonten müssen auch nicht gelöscht werden. Möchten betroffene Personen nicht mehr an dem Programm teilnehmen, genügt es, wenn der Zugang gesperrt wird. Das Risiko der Nutzung vorhandener Zugänge, wodurch in Beschwerden geltend gemachte Löschungsansprüche

häufig begründet wurden, besteht nicht. Außerdem wird das gesamte Kundenbindungsprogramm bisher von Mastercard nicht weiter betrieben und ist derzeit nicht erreichbar.

Durch die Bearbeitung sind sowohl bei Mastercard als auch bei mir in erheblichem Umfang Aufwände entstanden. Dies betrifft sowohl die Bearbeitung von Informationsanfragen als auch die Bearbeitung von Beschwerden und die Aufklärung des Sachverhalts. Der Vorgang macht deutlich, dass auch Sicherheitsmängel von vermeintlich geringem Umfang bei Veröffentlichung von personenbezogenen Daten zu einem erheblichen Aufwand und Reputationsschäden beim Verantwortlichen führen können. Aus dem Inhalt der Beschwerden, die bei mir eingereicht wurden, wird auch klar erkennbar, dass betroffene Personen einen signifikanten Vertrauensverlust in die von Mastercard betreute IT-Infrastruktur erlitten haben. Verantwortliche sollten daher ihre IT-Infrastruktur und die darin implementierten Sicherheitsmaßnahmen penibel überwachen und in allen kritischen Bereichen peinlich genau auf die Implementierung einer Zwei-Faktor-Authentisierung achten. Dies gilt in besonderem Maße für den Zugang von Administratoren.

11.3
Einheitliche Postbank ID für private und geschäftliche Konten

Private und geschäftliche Konten der Postbank können unter einer einheitlichen ID verwaltet werden. Durch die Einrichtung von Profilen / Sub-IDs wird eine hinreichende Trennung gewährleistet.

Die Verbindung von privaten und geschäftlichen Konten unter einer einheitlichen Postbank ID hat im Berichtszeitraum zu einigen datenschutzrechtlichen Beschwerden geführt. Bemängelt wurde insbesondere, dass eine hinreichende Trennung zwischen privaten und geschäftlichen Konten nicht gewährleistet sei. Beide Kontenarten würden zwangsweise miteinander verkoppelt.

Wenn etwa Beschäftigte auf dem heimischen Privat-PC Online-Banking betreiben, sei der unmittelbare Zugriff sowohl auf alle privaten als auch auf alle geschäftlichen Konten möglich. Dann könnten auch andere Familienmitglieder geschäftliche Konten des Arbeitgebers einsehen. Da das Direktionsrecht den Arbeitgeber nicht berechtigt, Anforderungen bzgl. Sicherheitsmaßnahmen für private PCs aufzustellen, sei fraglich, ob unter Risikogesichtspunkten in derartigen Fällen ein Zugriff über eine separate Postbank ID erforderlich sei.

Die Beschwerden waren Anlass für mich, das Verfahren näher zu betrachten. Dabei zeigte sich die Postbank kooperativ. Das Verfahren wurde mir in einem persönlichen Vor-Ort-Termin im Postbank Vertriebscenter in Wiesbaden

vorgestellt und erläutert. Ich konnte feststellen, dass – entgegen der Befürchtungen – eine hinreichende Trennung zwischen privaten und geschäftlichen Kontenzugriffen sichergestellt ist.

Im Einzelnen konnte ich feststellen, dass jeder Nutzer eine einheitliche Postbank ID erhält, mit welcher sowohl private als auch geschäftliche Konten verwaltet werden können. Diese Postbank ID verfügt als Erweiterung über sogenannte „Profile“ (Sub-IDs). Dabei handelt es sich um voreingestellte Filter zu den vergebenen Zugriffsberechtigungen. Jedem Nutzer wird zu jedem Kontoinhaber, auf dessen Konten zugegriffen wird, ein Profil zugeordnet. Nach dem Login mit Postbank ID und Passwort erhält der Nutzer für das angelegte geschäftliche Profil zunächst eine Mitteilung mit dem Namen des Profils und einer Anleitung für die Nutzung des Profils. Die zugeordneten Profile können in der Profilverwaltung verwaltet werden. Dort sind alle vorhandenen Profile – unterteilt nach privaten und geschäftlichen Profilen – aufgelistet. Buchungen können nur mit den zugehörigen Konten des jeweiligen Profils durchgeführt werden.

Ein Wechsel zwischen privaten und geschäftlichen Konten kann auf zwei verschiedene Arten geschehen, zum einen durch einen sog. „indirekten Wechsel“ und zum anderen durch einen sog. „direkten Wechsel“. Die gewünschte Variante kann in der Profilverwaltung festgelegt werden.

Als Standardeinstellung ist für einen Zugriff auf ein geschäftliches Konto ein „indirekter Wechsel“ vorgesehen. Das bedeutet, dass bei einem Login neben der Postbank ID auch der Profilname anzugeben ist, um die zugehörigen Konten einzusehen. Für einen Wechsel zu privaten bzw. geschäftlichen Konten müssen sich die Nutzer zunächst ausloggen und anschließend wieder neu einloggen. Diese Voreinstellung führt dazu, dass der Zugang zu privaten Konten nur über den Login mit der Postbank ID und für die geschäftlichen Konten nur mit der entsprechenden Erweiterung je Geschäftskonto möglich ist. Entsprechende Profile werden je nach Berechtigung automatisch für die betroffenen Kunden erstellt und diesen als Nachricht im Online-Banking als Vorschaltseite mitgeteilt. Zudem sind die entsprechenden Profile im Online-Banking in der Profilverwaltung zu finden. Diese Variante gewährleistet eine hinreichende Trennung zwischen geschäftlichen und privaten Konten und ist damit datenschutzrechtlich unproblematisch.

Beispiel: Herr Mustermanns Postbank ID lautet „Mustermann1“. Der Profilname des Unternehmens lautet „Unt“. Dann erfolgt der Login in das private Konto über „Mustermann1“ und in das geschäftliche Konto über „Mustermann1#Unt“. Das Passwort für das geschäftliche Konto ist dasselbe wie für das private Konto. Nach dem Login über „Mustermann1#Unt“ sieht Herr

Mustermann ausschließlich das geschäftliche Konto. Zudem erscheint der Hinweis „Angemeldet als #Unt“.

Es kann auch eingestellt werden, dass ein „direkter Wechsel“ zwischen privatem und geschäftlichem Profil stattfindet. Diese Einstellung müssen die Nutzer zunächst aktiv auswählen. Dabei ist ein gesonderter Login mit Postbank ID und Profilname nicht mehr notwendig. Um Profile über den direkten Wechsel zu erreichen, müssen die Nutzer nach dem Login mit der Postbank ID (ohne Profilnamen) auf das Profilsymbol und dann auf „Profil wechseln“ klicken. Anschließend klicken sie auf das entsprechende Profil. Es kann also ohne vorherigen Logout direkt zwischen geschäftlichem und privatem Konto gewechselt werden. Auch dann erfolgt eine getrennte Übersicht der geschäftlichen und privaten Konten. Wenngleich diese Variante ein datenschutzrechtlich geringeres Schutzniveau als der indirekte Wechsel bietet, ist gleichwohl noch eine hinreichende Trennung zwischen privaten und geschäftlichen Konten gewährleistet.

Geschäftskunden werden von der Postbank über das Verfahren der Postbank ID beraten. Wenn sowohl ein privates als auch ein geschäftliches Konto eines Kunden besteht, sollte es bei dem indirekten Kontenwechsel verbleiben.

Ich empfehle Arbeitgebern, dies grundsätzlich in einer betrieblichen Regelung für ihre Beschäftigten festzuhalten. Eine Nachfrage bei den einzelnen Beschäftigten, ob diese auch über ein privates Konto bei der Postbank verfügen, ist dagegen datenschutzrechtlich unzulässig.

11.4
Das Recht auf Löschung des Mandanten gegenüber dem Rechtsanwalt und die Aufbewahrungspflicht für Handakten

Das Recht auf Löschung personenbezogener Daten des Mandanten gegenüber seinem Rechtsanwalt gemäß Art. 17 Abs. 1 DS-GVO scheitert häufig an der rechtsanwaltlichen Aufbewahrungspflicht von sechs Jahren für Handakten gemäß § 50 Bundesrechtsanwaltsordnung i. V. m. Art. 17 Abs. 3 lit. b DS-GVO.

Mich haben Beschwerden erreicht, in denen Mandanten die Löschung der bei ihren Rechtsanwälten gespeicherten personenbezogenen Daten begehrten. Art. 17 Abs. 1 DS-GVO (Recht auf Löschung) gibt den betroffenen Personen und damit auch den Mandanten gegenüber ihren Rechtsanwälten grundsätzlich ein Recht auf Löschung ihrer personenbezogenen Daten. Allerdings besteht dieses Recht u. a. dann nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Art. 17 Abs. 3 lit. b DS-GVO

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist.

b) zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

§ 50 Bundesrechtsanwaltsordnung (BRAO) regelt eine solche rechtliche Verpflichtung, die das Recht auf Löschung personenbezogener Daten des Mandanten gegenüber dem Rechtsanwalt beschränkt.

§ 50 BRAO

(1) Der Rechtsanwalt muss durch das Führen von Handakten ein geordnetes und zutreffendes Bild über die Bearbeitung seiner Aufträge geben können. Er hat die Handakten für die Dauer von sechs Jahren aufzubewahren. Die Frist beginnt mit Ablauf des Kalenderjahres, in dem der Auftrag beendet wurde.

(2) Dokumente, die der Rechtsanwalt aus Anlass seiner beruflichen Tätigkeit von dem Auftraggeber oder für ihn erhalten hat, hat der Rechtsanwalt seinem Auftraggeber auf Verlangen herauszugeben. Macht der Auftraggeber kein Herausgabeverlangen geltend, hat der Rechtsanwalt die Dokumente für die Dauer der Frist nach Absatz 1 Satz 2 und 3 aufzubewahren. Diese Aufbewahrungspflicht gilt nicht, wenn der Rechtsanwalt den Auftraggeber aufgefordert hat, die Dokumente in Empfang zu nehmen, und der Auftraggeber dieser Aufforderung binnen sechs Monaten nach Zugang nicht nachgekommen ist. Die Sätze 1 bis 3 gelten nicht für die Korrespondenz zwischen dem Rechtsanwalt und seinem Auftraggeber sowie für die Dokumente, die der Auftraggeber bereits in Urschrift oder Abschrift erhalten hat.

(3) Der Rechtsanwalt kann seinem Auftraggeber die Herausgabe der Dokumente nach Absatz 2 Satz 1 so lange verweigern, bis er wegen der ihm vom Auftraggeber geschuldeten Gebühren und Auslagen befriedigt ist. Dies gilt nicht, soweit das Vorenthalten nach den Umständen unangemessen wäre.

(4) Die Absätze 1 bis 3 gelten entsprechend, sofern sich der Rechtsanwalt zum Führen von Handakten oder zur Verwahrung von Dokumenten der elektronischen Datenverarbeitung bedient.

(5) In anderen Vorschriften getroffene Regelungen zu Aufbewahrungs- und Herausgabepflichten bleiben unberührt.

§ 50 Abs. 1 Satz 2 sieht eine sechsjährige Aufbewahrungsfrist für Handakten des Rechtsanwalts vor. Im Hinblick auf elektronisch gespeicherte Daten gilt dies, soweit sich der Rechtsanwalt zum Führen der Handakten oder zur Verwahrung von Dokumenten der elektronischen Datenverarbeitung bedient, § 50 Abs. 4 BRAO.

Im Gesetzentwurf zur Umsetzung der Berufsanerkennungsrichtlinie und zur Änderung weiterer Vorschriften im Bereich der rechtsberatenden Berufe (BT-Drs. 18/9521 vom 05.09.2016, S. 115) wird zur aktuellen Fassung des § 50 Abs. 1 BRAO unter Bezugnahme auf die Löschungsverpflichtung der DS-GVO explizit ausgeführt, dass ein datenschutzrechtlicher Löschungsanspruch der Mandantschaft während der sechsjährigen Aufbewahrungsfrist ausgeschlossen ist.

Daher konnte ich den Petenten in diesen Fällen lediglich mitteilen, dass der Anspruch auf Löschung nicht besteht, soweit Handakten bzw. Dokumente auf Grundlage von § 50 BRAO beim Rechtsanwalt im Rahmen der Frist aufbewahrt werden.

11.5
Unverschlüsselte E-Mail-Kommunikation zwischen Rechtsanwalt und Mandant

Eine sichere Verarbeitung im Sinne der DS-GVO bedeutet grundsätzlich auch die Verschlüsselung personenbezogener Daten; das kann im Hinblick auf die elektronische Kommunikation den verschlüsselten Versand von E-Mails bedeuten. Das anwaltliche Berufsrecht sieht ab 01.01.2020 unter bestimmten Voraussetzungen jedoch vor, dass die unverschlüsselte E-Mail-Kommunikation zwischen Rechtsanwalt und Mandant – ohne Verstoß gegen die Berufspflicht zur Verschwiegenheit – zulässig sein soll.

Eine sichere Verarbeitung im Sinne der DS-GVO beinhaltet gemäß Art. 32 Abs. 1 lit. a DS-GVO (Sicherheit der Verarbeitung) grundsätzlich auch die Verschlüsselung personenbezogener Daten.

Art. 32 Abs. 1 lit. a DS-GVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten (…)

Im Hinblick auf die elektronische Kommunikation kann dies eine verschlüsselter E-Mail-Kommunikation erfordern. Ab 01.01.2020 sieht die Berufsordnung für Rechtsanwälte (BORA) in § 2 Abs. 2 BORA eine Erleichterung für die

elektronische Kommunikation zwischen Rechtsanwalt und Mandant vor (Beschluss der 6. Satzungsversammlung bei der Bundesrechtsanwaltskammer am 06.05.2019 zur Neufassung von § 2 BORA Verschwiegenheit).

§ 2 Abs. 2 BORA

(2) Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit der Vorschriften zum Schutz personenbezogener Daten deren Anforderungen entsprechen. Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen. Abs. 4 lit. c) bleibt hiervon unberührt. Zwischen Rechtsanwalt und Mandant ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, jedenfalls dann erlaubt, wenn der Mandant ihr zustimmt. Von einer Zustimmung ist auszugehen, wenn der Mandant diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat, fortsetzt.

Danach kann der Mandant auch einer unverschlüsselten E-Mail-Kommunikation ausdrücklich oder konkludent unter den in § 2 Abs. 2 Satz 4 und 5 BORA genannten Voraussetzungen zustimmen. Die Zustimmung des Mandanten kann jedoch nicht die personenbezogenen Daten Dritter umfassen.

Zudem hat das zuständige Bundesministerium der Justiz und für Verbraucherschutz darauf hingewiesen, dass der künftige § 2 Abs. 2 BORA die Regelungen DS-GVO nicht umgehen dürfe (Anwaltsblatt 2019, Verschwiegenheit: § 2 BORA neu, S. 528). Damit ist die Frage der Zulässigkeit unverschlüsselter E-Mail-Kommunikation zwischen Mandant und Rechtsanwalt lediglich in berufsrechtlicher Hinsicht beantwortet – die Frage der datenschutzrechtlichen Zulässigkeit nach der DS-GVO ist damit noch nicht geklärt. Allerdings kann die neue berufsrechtliche Regelung künftig in die datenschutzrechtliche Bewertung mir vorliegender konkreter Sachverhalte mit einbezogen werden.

Im Übrigen hat meine Behörde gemäß § 29 Abs. 3 BDSG nur eingeschränkte Untersuchungsbefugnisse gegenüber Rechtsanwälten, so dass eine allgemeine Prüfung der Kommunikationswege in der Regel – insbesondere bei Beschwerden Dritter – nicht möglich ist.

12. Inkasso, Auskunfteien

12.1
Umsetzung der DS-GVO durch die SCHUFA Holding AG

Die Verarbeitung von Bonitätsinformationen durch die SCHUFA Holding AG (SCHUFA) hat auf betroffene Personen in der Regel erhebliche Auswirkungen. Enthalten Bonitätsinformationen der SCHUFA einen Hinweis auf eine eingeschränkte Bonität, ist die Teilnahme am Wirtschaftsleben üblicherweise ebenfalls eingeschränkt. Deshalb unterziehe ich die SCHUFA einer verschärften Kontrolle.

Die Bonitätsauskünfte greifen besonders intensiv in die wirtschaftlichen Interessen der Betroffenen ein. Die DS-GVO enthält deshalb strenge Vorgaben. Das führte dazu, dass sich die SCHUFA nachhaltig auf die Geltung der DS-GVO vorbereiten musste.

Bereits 2016 haben sich die Aufsichtsbehörden intensiv mit den Auswirkungen der DS-GVO auf die Datenverarbeitung der Wirtschaftsauskunfteien befasst. In mehreren Sitzungen wurden die wichtigsten Fragen behandelt und, soweit dies möglich war, eine bundeseinheitliche Auffassung abgestimmt. Dies betraf vor allem die Zulässigkeit der Datenverarbeitung inklusive des Scorings durch Wirtschaftsauskunfteien nach der DS-GVO, die von allen Aufsichtsbehörden für weiterhin gegeben erachtet wurde. Darüber hinaus betraf es die sich aus der DS-GVO ergebenden Informationspflichten und die von Wirtschaftsauskunfteien zu erteilenden Auskünfte. Die Informationen waren aufgrund der Regelungen in den Artikeln 13 und 14 DS-GVO anzupassen und zu erweitern. Außerdem mussten die von der SCHUFA erteilten Selbstauskünfte angepasst werden. Die nach der DS-GVO notwendigen Maßnahmen wurden mit mir abgestimmt und von der SCHUFA vollständig umgesetzt.

Die wesentlichste Auswirkung, die von der SCHUFA durch eine aufwändige Änderung des Prozesses umzusetzen war, betraf die Rechtsgrundlage für die Übermittlung von Daten an die SCHUFA und die Erteilung von Auskünften. Vor dem Wirksamwerden der DS-GVO wurde von Vertragspartnern der SCHUFA durch Verwendung eines als „SCHUFA Klausel“ bekannten Vertragsbestandteils eine Einwilligung zur Übermittlung von Daten an die SCHUFA eingeholt. Da diese Einwilligung in den weitaus meisten Fällen auch eine Voraussetzung für das Aufnehmen von Vertragsverhandlungen war, hätte dieses Vorgehen gegen die notwendige Freiwilligkeit einer Einwilligung gemäß Art. 7 DS-GVO verstoßen. Die Wirksamkeit der Einwilligung wäre daher mehr als zweifelhaft gewesen.

Aufgrund dessen war das Verfahren umzustellen und auf die Einholung einer Einwilligung zu verzichten. Nach Auffassung aller Aufsichtsbehörden bildet bereits Art. 6 Abs. 1 lit. f) DS-GVO eine ausreichende Rechtsgrundlage für die Verarbeitung von Daten durch Wirtschaftsauskunfteien. Eine Einwilligung ist daher nicht erforderlich. Wird auf die Einholung einer Einwilligung verzichtet, ist außerdem sichergestellt, dass die Datenverarbeitung durch Wirtschaftsauskunfteien ausschließlich im Rahmen der gesetzlichen Regelungen erfolgt. Die Umstellung ist daher für betroffene Personen vorteilhaft.

Die SCHUFA hat daraufhin das Verfahren umgestellt und verzichtet zum Vorteil aller betroffenen Personen seit dem Wirksamwerden der DS-GVO auf die Einholung einer Einwilligung.

Durch das Wirksamwerden der DS-GVO ist außerdem die Vorschrift des § 35 Abs. 2 Satz 2 Nr. 4 BDSG (alt) entfallen, nach der Daten durch Wirtschaftsauskunfteien in der Regel nach dem Ende des dritten Jahres nach Speicherung zu löschen waren. Aufgrund des Fristbeginns erst am Ende des Jahres, in dem die Speicherung erfolgt war, dauerte die Speicherung in aller Regel erheblich länger als drei Jahre. Gleichwohl bestand mit § 35 Abs. 2 Satz 2 Nr. 4 BDSG (alt) eine eindeutige gesetzliche Regelung über die Speicherdauer von Daten, die durch Wirtschaftsauskunfteien gespeichert wurden.

Mangels gesetzlicher Regelung musste mit den Wirtschaftsauskunfteien eine neue Speicherfrist festgelegt werden. Gemäß Art. 17 Abs. 1 lit. a) DS-GVO sind Daten zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr notwendig sind. Zweck der Speicherung von Daten durch Wirtschaftsauskunfteien ist die Prüfung der Bonität betroffener Personen. Durch Wirtschaftsauskunfteien verarbeitete Bonitätsinformationen müssen daher spätestens dann gelöscht werden, wenn sie keine belastbare Aussagekraft für die Bonität mehr haben. Die Wirtschaftsauskunfteien konnten nachweisen, dass Bonitätsinformationen für einen Zeitraum von mindestens drei Jahren eine belastbare Aussage zur Bonität betroffener Personen ermöglichen. Aufgrund dessen haben die Wirtschaftsauskunfteien durch ihren Verband „Die Wirtschaftsauskunfteien e. V." Verhaltensregeln gemäß Art. 40 DS-GVO entworfen, in denen eine Speicherfrist von drei Jahren festgelegt wurde. Die darin enthaltene Frist beginnt mit der Speicherung der Daten. Daten werden daher bereits exakt drei Jahre nach Erledigung des Ereignisses, auf das sie sich beziehen, gelöscht. Die Speicherdauer wurde damit gegenüber der bisherigen Speicherdauer erheblich verkürzt.

Diese als „Code auf Conduct" bezeichneten und auf der Internetpräsenz http://www.handelsauskunfteien.de abrufbaren Verhaltensregeln wurden nicht zuletzt wegen der verkürzten Speicherdauer durch die für den Verband „Die Wirtschaftsauskunfteien e. V." zuständige Landesbeauftragte für Da-

tenschutz und Informationsfreiheit Nordrhein-Westfalen in Abstimmung mit den anderen Aufsichtsbehörden genehmigt. Dadurch werden für betroffene Personen eine verkürzte Speicherdauer und Rechtssicherheit geschaffen.

12.2
Die Speicherung von Daten zur Durchführung eines Insolvenzverfahrens nach erteilter Restschuldbefreiung durch Auskunfteien

Die Aussagekraft von Daten zur Durchführung eines Insolvenzverfahrens hinsichtlich der Bonität der betroffenen Personen rechtfertigt die Datenspeicherung durch Auskunfteien auch nach einer bereits erteilten Restschuldbefreiung.

Eine Vielzahl eingehender Beschwerden hat zum Gegenstand, dass Auskunfteien Daten zur Durchführung eines Insolvenzverfahrens auch nach Erteilung einer Restschuldbefreiung speichern. Die Speicherung von Einträgen zu abgeschlossenen Privatinsolvenzen schränkt die Teilnahme am Wirtschaftsleben üblicherweise ein und impliziert Probleme, die die betroffenen Personen in vielen Fällen mit der Erteilung der Restschuldbefreiung für überwunden gehalten haben.

Gemäß Art. 5 Abs. 1 lit. e) DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie dies für den mit der Speicherung verbundenen Zweck erforderlich ist. Entfällt die Erforderlichkeit, ist der Verantwortliche gemäß Art. 17 Abs. 1 lit. a) DS-GVO zur Löschung der Daten verpflichtet. Im Hinblick auf die Speicherdauer für Daten aus Insolvenzverfahren existiert jedoch keine konkrete gesetzliche Regelung.

Der mit der Speicherung von Daten aus Insolvenzverfahren verfolgte Zweck besteht in der Beurteilung der Bonität betroffener Personen. Folglich sind Daten aus Insolvenzverfahren spätestens dann zu löschen, wenn sich von ihnen keine belastbare Aussagekraft mehr für die Bonität ableiten lässt. Personen, die ein Privatinsolvenzverfahren durchlaufen haben, geraten nachweislich häufiger erneut in Zahlungsschwierigkeiten als andere Personen. Dies lässt sich auch auf die eingeschränkte Möglichkeit zum Aufbau von Rücklagen während des Insolvenzverfahrens zurückführen. Die sich daraus ergebende Aussagekraft von Daten zu Insolvenzverfahren für einen nicht unerheblichen Zeitraum rechtfertigt die Speicherung auch nach Beendigung eines Insolvenzverfahrens.

Im Rahmen von freiwilligen Verhaltensregeln für Auskunfteien wurde die Speicherdauer für Daten aus Insolvenzverfahren vereinheitlicht und kon-

kretisiert. Auf Grundlage des sog. „Code of Conduct“ des Verbandes „Die Wirtschaftsauskunfteien e. V.“ haben sich die Auskunfteien dazu verpflichtet, personenbezogene Daten aus Insolvenz- oder Restschuldbefreiungsverfahren taggenau drei Jahre nach deren Beendigung bzw. nach Erteilung der Restschuldbefreiung zu löschen. Der „Code of Conduct“ wurde von den Datenschutzaufsichtsbehörden geprüft und als gesetzeskonform beurteilt. Demnach besteht kein Anspruch auf eine frühere Löschung entsprechender Daten.

Es ist zu berücksichtigen, dass sich Daten aus Insolvenzverfahren mit fortschreitender Dauer immer weniger auf die Bonität auswirken. Je länger eine Restschuldbefreiung zurückliegt, desto besser entwickelt sich die durchschnittliche Bonität der betroffenen Personen. Im Ergebnis verbessert sich damit einhergehend gleichfalls ein von einer Auskunftei berechneter Scorewert in der Regel stetig mit einem zunehmenden zeitlichen Abstand zu der Erteilung einer Restschuldbefreiung.

13. Internet

13.1
Datenschutz bei neuen Internetdiensten

Bei der Entwicklung und Ausgestaltung neuer, innovativer Internetdienste sollte von Anfang an auch das Datenschutzrecht beachtet werden. Andernfalls besteht die Gefahr, dass schwer aufzulösende Datenschutzprobleme entstehen, die umfangreiche Änderungen erfordern oder sogar den Betrieb des Dienstes gefährden können.

Durch eine Presseanfrage sowie Berichte in verschiedenen Medien wurde ich auf einen von einem Startup-Unternehmen angebotenen Dienst aufmerksam, der dem Schutz von Kindern bei der Kommunikation über das Internet dienen sollte. Das Startup-Unternehmen hatte mittels künstlicher Intelligenz (KI) ein System entwickelt, das schriftliche Kommunikation über das Internet (z. B. via Instant-Messenger) analysieren und darin Inhalte erkennen konnte, die für Kinder problematisch sein können.

Mittels dieser Technik bot das Unternehmen einen App-basierten Dienst an, der für Kinder und Jugendliche potenziell gefährliche Kommunikation bzw. Kommunikationspartner (z. B. Cybergrooming, Sexting etc.) erkennen konnte und die Erziehungsberechtigten auf die konkrete Gefahr hinwies. Die Eltern konnten sich bei dem Dienst kostenpflichtig anmelden und eine Verbindung zwischen dem Dienst und einer auf dem Handy des Kindes installierten App eines bestimmten, weit verbreiteten Messengers herstellen. Dazu wurde eine Schnittstelle ausgenutzt, die der Anbieter des Messengers für dessen Webbasierte Nutzung zur Verfügung stellt. Sobald diese Verbindung bestand, wurde die gesamte über diesen Messenger geführte Kommunikation des Kindes auf die Server des Diensteanbieters übertragen und dort von der KI analysiert. Sofern der Algorithmus Hinweise darauf fand, dass die Kommunikation für das Kindeswohl gefährlich sein könnte, wurden die Erziehungsberechtigten auf diesen Umstand hingewiesen und zur Überprüfung des Vorgangs und Unterstützung des Kindes aufgefordert.

Obwohl der Zweck dieses Dienstes selbstverständlich begrüßens- und unterstützenswert ist, barg dessen Ausgestaltung auch erhebliche Risiken für das Persönlichkeitsrecht der Betroffenen.

Aus datenschutzrechtlicher Sicht problematisch war der Dienst insbesondere dadurch, dass die gesamte per Messenger geführte Kommunikation automatisch an den Diensteanbieter weitergeleitet und von diesem gespeichert und verarbeitet wurde. Dies betraf notwendigerweise nicht nur die Kommunikation des von seinen eigenen Eltern überwachten Kindes, sondern auch

die von dessen verschiedenen Chatpartnern. Die elektronisch geführten Unterhaltungen fallen sowohl unter das Telekommunikationsgeheimnis als auch unter das Datenschutzrecht, da die Chats regelmäßig eine Vielzahl personenbezogener Daten enthalten und zudem Meta-Daten (z. B. Zeitpunkt der Kommunikation etc.) anfallen.

Erschwerend kommt hinzu, dass der Dienst explizit der Überwachung Minderjähriger diente, deren Chatpartner zumeist andere Minderjährige sind. Kinder und Jugendliche genießen im Datenschutzrecht besonderen Schutz, da sie regelmäßig noch nicht in der Lage sind, die mögliche Tragweite von Datenverarbeitungsvorgängen zu erfassen.

In der vorliegenden Konstellation ist es bereits schwierig, die Verarbeitung der Daten bzw. Kommunikationsinhalte desjenigen Kindes, dessen Erziehungsberechtigte den Dienst nutzen, datenschutzrechtlich in zulässiger Weise zu gestalten. Da anderweitige Rechtsgrundlagen dazu nicht in Betracht kommen, können die Daten nur mit der Einwilligung des betroffenen Kindes verarbeitet werden. Dabei hängt es jedoch vom Alter und der Einsichtsfähigkeit des Kindes ab, ob dieses selbst in die Datenverarbeitung einwilligen kann oder ob die Eltern als Erziehungsberechtigte dies für das Kind tun können bzw. müssen. In diesem Zusammenhang stellen sich zudem Fragen der Transparenz und der Hinweispflichten gegenüber dem Kind. Auch sind verschiedene technische Datenschutzanforderungen (z. B. Verschlüsselung, sichere Speicherung, fristgerechte Löschung etc.) zu beachten.

Noch problematischer ist jedoch die Tatsache, dass auch die gesamte Kommunikation der Chatpartner eines überwachten Kindes an den Diensteanbieter weitergeleitet und dort verarbeitet wurde. Ohne Zutun des überwachten Kindes bzw. der Eltern, die den Dienst zum Schutze ihres Kindes nutzten, konnten die Chatpartner jedoch nicht einmal erkennen, dass der Dienst überhaupt genutzt wurde und ihre gesamte Kommunikation mit dem überwachten Kind automatisch an ein für sie unbekanntes Unternehmen übermittelt und dort verarbeitet wurde. Ohne dieses Wissen war es für die Kommunikationspartner auch nicht möglich, dem Dienst auszuweichen, geschweige denn in hinreichender Form und nach erfolgter Information in die Verarbeitung ihrer Daten wirksam einzuwilligen. Es hätte vermutlich erhebliche Veränderungen an dem Dienst erfordert, um eine datenschutzrechtlich tragfähige Lösung für dieses Problem umzusetzen.

Die Beantwortung bzw. Lösung dieser datenschutzrechtlich problematischen Fragen konnte im konkreten Fall letztlich jedoch dahinstehen, da der Dienst aus finanziellen Gründen vom Anbieter eingestellt wurde. Damit wurde auch die zu diesem Zeitpunkt noch laufende Datenschutzprüfung gegenstandslos.

Das vorliegende Beispiel zeigt allerdings, dass selbst der noch so gute und begrüßenswerte Wunsch, Kinder vor bestimmten Gefahren bei der Internetnutzung zu schützen, ungewollt auch mit einer nicht unerheblichen Gefährdung für die Persönlichkeitsrechte der Kinder und unbeteiligter Dritter einhergehen kann. Entwickler von neuen, innovativen Diensten tun deshalb gut daran, bereits bei der Entwicklung der Dienste deren datenschutzrechtliche Folgen zu bedenken und die Dienste so zu gestalten, dass die Persönlichkeitsrechte der Nutzer dadurch nicht beeinträchtigt werden.

13.2
Cookies, Plugins & Tools: Was gilt für ihren Einsatz?

In nahezu jedem internetbasierten Dienst sind heute verschiedene kleine Dienste und Tools eingebunden, die nicht vom Betreiber des Dienstes selbst, sondern von anderen Unternehmen angeboten und betrieben werden. Sehr häufig werden insbesondere Dienste zur Webanalyse, Werbenetzwerke und Plugins zur Einbindung externer Inhalte eingesetzt. Viele dieser Dienste sind allerdings datenschutzrechtlich problematisch.

Es gibt eine Vielzahl von verschiedenen Tools, die die Betreiber von internetbasierten Diensten (z. B. Webseiten, Mobil-Apps, Smarte Geräte etc.) in ihre Angebote einbinden können, um verschiedene zusätzliche Funktionen für sich und/oder ihre Nutzer zu erhalten. So werden beispielsweise oft Dienste zur Webanalyse genutzt, mittels derer die Diensteanbieter genauere Informationen über die tatsächliche Nutzung ihrer Angebote erlangen, um diese optimieren und anpassen zu können. Viele Betreiber setzen zudem Werbenetzwerke ein, um das eigene Angebot auch auf anderen Webseiten bzw. Portalen bewerben zu können. Häufig werden auch externe Inhalte (z. B. Videos, Karten, interaktive Elemente), Dienste (z. B. Zahlungsdienste) oder Social Plugins (z. B. Like Button) eingebunden. Solche Dienste und Tools werden in aller Regel nicht vom Anbieter eines Internetdienstes selbst, sondern von spezialisierten Unternehmen angeboten und betrieben und sind heute in einem Großteil aller internetbasierter Dienste eingebunden.

Verantwortlichkeit

Grundsätzlich ist jeder Anbieter eines Internetdienstes für die darüber anfallenden Nutzerdaten selbst verantwortlich. Die meisten der o. g. Dienste von Drittanbietern erheben und verarbeiten jedoch ebenfalls personenbezogene Daten der Nutzer bzw. setzen die Übermittlung dieser Daten durch den Diensteanbieter voraus. Insbesondere ist für die Funktion vieler dieser Drittanbieter-Dienste die (häufig diensteübergreifende) Wiedererkennbarkeit

eines bestimmten Nutzers entscheidend (sog. Tracking). Für den Anbieter eines Dienstes, der Tools von Dritten einsetzt, spielt der Umfang der Datenverarbeitung bei diesen häufig nur eine untergeordnete Rolle, da es ihm im Wesentlichen auf die Erreichung des Zwecks des jeweils eingesetzten Tools (z. B. Einbindung eines Videos, bessere Vermarktung, Webanalyse usw.) ankommt. Dennoch wird der Anbieter durch die Einbindung solcher Drittanbieter-Dienste regelmäßig datenschutzrechtlich mitverantwortlich für die von diesen vorgenommenen Datenverarbeitungen, da auf seine Veranlassung Daten seiner Nutzer automatisch an die Anbieter übermittelt werden.

Hintergrund

Schon nach der alten Rechtslage vor Inkrafttreten der DS-GVO waren die rechtlichen Voraussetzungen für die Einbindung solcher Dienste keineswegs eindeutig. Mit Gültigkeit der DS-GVO seit Mai 2018 ist die Rechtslage allerdings noch unklarer geworden. Ursprünglich sollte zeitgleich mit der DS-GVO die europäische ePrivacy-Verordnung in Kraft treten, mit der der europäische Gesetzgeber spezielle Regeln zur Datenverarbeitung in der elektronischen Kommunikation festlegen wollte. Aus politischen Gründen hat sich das Gesetzgebungsverfahren jedoch über Jahre hingezogen und scheint inzwischen sogar, zumindest vorerst, gescheitert zu sein. Dadurch sind derzeit viele Fragen des Datenschutzes in der elektronischen Kommunikation ungeregelt bzw. ungeklärt. Die daraus resultierende Unsicherheit bei den Verantwortlichen und den Betroffenen zeigt sich eindrücklich auch in der großen Anzahl an Beschwerden und Beratungsanfragen, die mich im Berichtszeitraum diesbezüglich erreicht haben.

Rechtslage / Orientierungshilfe für Anbieter von Telemedien

Zur Erläuterung der geltenden Rechtslage und um die Ansichten der Aufsichtsbehörden zu diesem Thema darzulegen, hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im März 2019 die „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ verabschiedet (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf). Diese enthält ausführliche Erläuterungen dazu, welche datenschutzrechtlichen Regeln nach Ansicht der Aufsichtsbehörden bei der Verarbeitung von Nutzungsdaten in der elektronischen Kommunikation derzeit anwendbar sind und welche Voraussetzungen für den Einsatz der o. g. Dienste gelten.

Da die bisherigen Regeln zur Verarbeitung von Nutzerdaten aus dem Telemediengesetz (TMG) aufgrund des Vorrangs der DS-GVO nicht mehr angewendet werden können und es keine sonstigen, spezielleren Vorschriften gibt,

ist derzeit ausschließlich die DS-GVO für die Verarbeitung von Nutzerdaten heranzuziehen.

Danach kann die Nutzung von Drittanbieter-Tools in bestimmten Fällen auf die Rechtsgrundlage des Art. 6 Abs. 1 S. 1 lit. f DS-GVO gestützt werden und somit auch ohne Zustimmung des Nutzers zulässig sein. Dies ist jedoch nur möglich, wenn die Verarbeitung der Nutzerdaten durch den jeweiligen Dienst in relativ geringem Maße in die Rechte des Nutzers eingreift und dessen Interessen die des Diensteanbieters nicht deutlich überwiegen. Im Rahmen der dabei vorzunehmenden Interessenabwägung sind verschiedene Faktoren wie z. B. Transparenz, Widerspruchsmöglichkeit des Nutzers, Umfang der Datenverarbeitung, Zahl der Beteiligten etc. zu berücksichtigen. Somit können bei entsprechend datenschutzfreundlichen Einstellungen auf dieser Rechtsgrundlage beispielsweise Dienste zur Webanalyse, die ohne angebotsübergreifendes Tracking auskommen, genutzt oder externe Inhalte Dritter eingebunden werden, wenn dies ohne Verfolgung der Nutzeraktivitäten durch den Dritten einhergeht.

Bei Internetdiensten, die von öffentlichen Stellen angeboten werden (z. B. Webseiten von Behörden), ist die Verarbeitung von Nutzerdaten nur dann zulässig, wenn sie gem. Art. 6 Abs. 1 S. 1 lit. e DS-GVO für die Wahrnehmung der öffentlichen Aufgabe der Stelle erforderlich ist. Während Internetauftritte für die Öffentlichkeitsarbeit sowie bestimmte inhaltliche Online-Angebote (z. B. E-Government) von Behörden regelmäßig erforderlich sind, ist dies beim Einsatz von Drittanbieter-Tools jedoch in der Regel nicht der Fall.

Viele Tools von Drittanbietern verarbeiten Nutzerdaten allerdings in einer Weise bzw. in einem Umfang, die mit Art. 6 Abs. 1 S. 1 lit. f DS-GVO nicht in Einklang zu bringen ist. Dies betrifft insbesondere viele Tools zur Webanalyse, Social-Plugins sowie nahezu alle Anbieter von nutzungsbasierter Werbung. Der Einsatz dieser Dienste ist nur zulässig, wenn der jeweilige Nutzer darin ausdrücklich eingewilligt hat. Das Einholen einer datenschutzrechtlich wirksamen Einwilligung erweist sich in der Praxis allerdings als schwierig. Dazu ist es u. a. erforderlich, dass die Nutzer ausreichend über die Datenverarbeitung informiert werden und dass die Einwilligung freiwillig und ohne Zwang abgegeben sowie durch eine aktive Handlung des Nutzers erklärt wird. Das reine Weiternutzen eines Angebots, das Wegklicken von Bannern mit der „Schließen"-Schaltfläche oder vorausgewählte Kästchen mit Einwilligungserklärungen genügen insoweit nicht. Zudem dürfen die Dienste und Tools, in deren Nutzung eingewilligt werden soll, erst nach der erfolgten Einwilligung geladen bzw. in den Internetdienst eingebunden werden.

Fazit

Derzeit fallen Rechtslage und Wirklichkeit bei solchen erforderlichen Einwilligungen häufig noch auseinander. Seit Inkrafttreten der DS-GVO setzen zwar immer mehr Internetdienste sog. Cookie-Banner und/oder Consent-Management-Tools ein, deren Inhalt und technische Funktion sind aber häufig sehr zweifelhaft und nicht ausreichend. Es bleibt zu hoffen, dass der Gesetzgeber doch noch klare Regeln für den Datenschutz in der elektronischen Kommunikation aufstellt oder zumindest durch höchstrichterliche Urteile einige der offenen Fragen geklärt werden und so mehr Rechtssicherheit geschaffen wird.

13.3
Identifizierungsverfahren von Online-Portalen

Identifizierungsverfahren von Online-Portalen müssen ein angemessenes Sicherheitsniveau gegen unberechtigte Ausleseversuche aufweisen.

Mich erreichte in diesem Jahr eine Beschwerde gegen ein Unternehmen, das dem Kunden die Möglichkeit gibt, seine Daten im Internet einzusehen. Der Beschwerdeführer legte dar, dass sämtliche personenbezogene Daten per Online-Link ins Internet gestellt seien. Um auf die Daten zuzugreifen, seien lediglich 5-stellige alphanumerische Zeichen notwendig, die an eine URL angehängt werden. Die Aktenzeichennummer zum Vorgang erscheine nach dem Aufruf der URL automatisch. Als Passwort würde die Postleitzahl des Kunden erfragt. Die für die Anmeldung erforderlichen Daten, URL und Postleitzahl samt Aktenzeichen werden als verschlossener kuvertierter Brief zur Verfügung gestellt. Der Beschwerdeführer bemängelte, dass nach Aufruf der URL als Passwort ausschließlich die Postleitzahl abgefragt werde und somit ein hohes Sicherheitsrisiko bestehe.

Ich habe das Unternehmen zur Stellungnahme aufgefordert und den Sachverhalt sowie die organisatorischen und technischen Maßnahmen in einem Vorortttermin überprüft.

Dabei stellte ich fest, dass die individuelle Kurz-URL tatsächlich mit nur fünf angehängten Zeichen zum Schluss verwendet und durch die weitere Abfrage der Postleitzahl gesichert wird. Diese Konzeption allein ist aus Sicherheitsgründen nicht ausreichend, weil zu kurz und zu leicht zu überwinden. Erfahrungen aus der Vergangenheit zeigen, dass gegen Kurz-URLs sogenannte Brute-Force-Angriffe einfach durchzuführen sind. Entsprechendes gilt für das Auslesen der Postleitzahl.

Die Brute-Force-Methode ist eine beliebte Methode, um Passwörter oder Daten herauszufinden. Dazu probiert sie automatisiert wahllos verschiedene

Buchstabenfolgen oder Zeichenketten aus. Mit steigender Komplexität und Länge der URL steigt die Anzahl an benötigten Rechenoperationen für den Brute-Force-Angriff.

Für ein erhöhtes Schutzniveau sind deshalb normalerweise mindestens zehn bis zwölf Zeichen vorzusehen.

Durch meine Kontrolle konnte ich allerdings auch feststellen, dass im vorliegenden Fall weitere Sicherheitsmaßnahmen getroffen wurden, so dass in der Gesamtschau die Sicherungsmaßnahmen aus datenschutzrechtlicher Sicht ausreichten. So war die Kurz-URL zufallsgeneriert und wurde sofort auf 7-stellig erweitert. Um einen Brute-Force-Angriff zum Scheitern zu bringen, waren Sicherheitsmaßnahmen zudem so gesetzt, dass eine automatisierte Überwachung der Anzahl der Anmeldeversuche mit einer Netzwerküberwachungssoftware erfolgte, die umgehend anschlägt, wenn diese Anzahl das Übliche erheblich übersteigt. In diesem Fall wird ein Angriff unterstellt, die Webseite vom Netz getrennt und die jeweiligen IT-Verantwortlichen des Unternehmens unverzüglich informiert. Selbst für den unwahrscheinlichen Fall, dass ein Angreifer eine zutreffende Login-Seite herausfindet, sind weitere IT-Sicherheitsmaßnahmen implementiert, die ein Ausprobieren von Anmeldungsdaten unterbindet bzw. meldet und ggf. den Eintrag sperrt.

Im Ergebnis waren die getroffenen organisatorischen und technischen Maßnahmen auf einem angemessenen Schutzniveau. Insbesondere die Überwachung der Anzahl der Anmeldeversuche ist aus meiner Sicht unverzichtbar, um ein angemessenes Sicherheitsniveau zu gewährleisten.

13.4
Datenschutzkonformer Einsatz von Web-basierten Chat-Applikationen

Auf zahlreichen, über das Internet zugreifbaren Websites werden Besucherinnen und Besuchern Chat-Funktionalitäten angeboten. Eine minimalistische Benutzerschnittstelle suggeriert häufig ein klares und einfaches Kommunikationskonzept, während im Hintergrund diverse begleitende Prozesse ablaufen. Bei der Bereitstellung derartiger und vergleichbarer Funktionalitäten müssen Verantwortliche ein besonderes Augenmerk auf die rechtmäßige und transparente Verarbeitung personenbezogener Daten nach Treu und Glauben gemäß Art. 5 Abs. 1 lit. a DS-GVO richten.

Im Frühjahr des Berichtszeitraums erreichte mich eine Beschwerde gegen die Chat-Funktionalität auf der Webseite eines Finanzdienstleisters. Über diese Chat-Funktionalität hatten die Besucher der Website die Möglichkeit,

mit Mitarbeiterinnen und Mitarbeitern des Dienstleisters in Kontakt zu treten und sich bspw. über dessen Angebote zu informieren.

Die Benutzerschnittstelle der beanstandeten Chat-Funktionalität war sehr einfach aufgebaut. Nach der Eingabe eines frei wählbaren Namens gelangten die Benutzer auf die eigentliche Chat-Oberfläche. Auf dieser standen ihnen neben einem Eingabefeld für Nachrichten auch eine Absenden-Schaltfläche für den Versand der Nachrichten zur Verfügung. Die ausgetauschten Nachrichten konnten über einen Gesprächsverlauf eingesehen werden. Der Aufbau der Benutzerschnittstelle orientierte sich offensichtlich in vereinfachter Form an denen gängiger Messenger-Applikationen.

Für eine derartige Chat-Funktionalität ist davon auszugehen, dass die Benutzer erwarten, dass sie ihre Chat-Nachrichten im dafür vorgesehenen Eingabefeld erstellen und ggf. korrigieren können, sowie dass eine von ihnen erstellte Chat-Nachricht ausschließlich bei Betätigung der Absenden-Schaltfläche an den Kommunikationspartner übermittelt wird. Erst mit Betätigen einer solchen Schaltfläche ist ferner davon auszugehen, dass ein Benutzer in die Übermittlung der personenbezogenen Daten aus dem Eingabefeld einwilligt.

Der Petent führte in seiner Beschwerde an, dass Chat-Nachrichten nicht erst durch Betätigung der Absenden-Schaltfläche übermittelt werden würden. Vielmehr würden nicht zur Übermittlung vorgesehene Chat-Nachrichten unmittelbar nach der Eingabe einzelner Buchstaben an den Finanzdienstleister übermittelt, ohne dass die Benutzerin oder der Benutzer hiervon in Kenntnis gesetzt werde. Für seine Behauptungen lieferte der Petent entsprechende Belege.

Als Reaktion auf die Beschwerde führte ich in meinem IT-Laboratorium eine technische Prüfung die Chat-Funktionalität durch. Im Ergebnis konnte ich den Vorwurf des Petenten auch auf der technischen Ebene des Transfer-Protokolls nachvollziehen. Die Chat-Funktionalität auf der Website des Finanzdienstleisters war so eingerichtet, dass Änderungen im Eingabefeld für Chat-Nachrichten nahezu in Echtzeit an den Finanzdienstleister übermittelt wurden. Eine Betätigung der Absenden-Schaltfläche war hierzu nicht erforderlich. Diese Übermittlung personenbezogener Daten war für Benutzer in der Web-Oberfläche der Chat-Funktionalität in keiner Weise ersichtlich. Auf Basis der Resultate der technischen Analysen kam ich zu dem Ergebnis, dass die Chat-Funktionalität in dieser Form nicht DS-GVO konform war. Sie verstieß gegen den Grundsatz, dass personenbezogene Daten gemäß Art. 5 Abs. 1 lit. a DS-GVO in einer für den Benutzer nachvollziehbaren Weise verarbeitet werden müssen. Im vorliegenden Fall war für die Verarbeitung personenbezogenen Daten im Rahmen der Chat-Funktionalität außerdem eine Einwilligung der betroffenen Person gemäß Art. 6 Abs. 1 lit. a DS-

GVO erforderlich. Eine solche Einwilligung lag für die ohne Betätigung der Absenden-Schaltfläche übermittelten personenbezogenen Daten nicht vor.

Ich forderte den Finanzdienstleister daraufhin zu einer Stellungnahme auf. Der Finanzdienstleister teilte mir mit, dass er meine rechtliche Auffassung hinsichtlich der erforderlichen Einwilligung gemäß Art. 6 Abs. 1 lit. a DS-GVO und deren Fehlen im Falle der fraglichen Datenübermittlung teile. Ferner teilte er mir mit, dass die beanstandete Teilfunktionalität zwischenzeitlich deaktiviert worden sei und somit eine Datenübermittlung im Kontext der Chat-Funktionalität nur noch durch Betätigung der Absenden-Schaltfläche durch die Benutzer erfolge.

Im Rahmen der Klärung des Sachverhalts stellte sich heraus, dass der Finanzdienstleister als Grundlage seiner Chat-Funktionalität keine Individualentwicklung einsetzte, sondern das Produkt eines Herstellers verwendete. Der Hersteller bewarb die beanstandete Teilfunktionalität für dieses Produkt explizit auf seiner Website. Für den datenschutzkonformen Einsatz dieser und ähnlicher Teilfunktionalitäten trägt jedoch im konkreten Fall ein Verantwortlicher gemäß Art. 24 DSGVO die Verantwortung. Daher sollten Verantwortliche bereits bei der Auswahl von Produkten und Dienstleistungen, in deren Kontext personenbezogene Daten verarbeitet werden, ein besonderes Augenmerk auf eine datenschutzkonforme Einsetzbarkeit derselben richten. Nach deren Auswahl bilden die konkrete Konfiguration und die Ausgestaltung des Einsatzkontextes weitere wesentliche Bausteine im Zusammenhang mit dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung gemäß Art. 25 DS-GVO.

Da durch den Einsatz der beanstandeten Teilfunktionalität der Grundsatz des Art. 5 Abs. 1 lit. a DS-GVO nicht beachtet wurde und darüber hinaus erforderliche Einwilligungen gemäß Art. 6 Abs. 1 lit. a DS-GVO nicht vorlagen, liegt ein Verstoß im Sinne des Art. 83 Ab. 5 lit. a DS-GVO vor. Die Verarbeitung von personenbezogenen Daten wie im vorliegenden Fall kann einen Bußgeldbestand erfüllen und wird deshalb nach Abschluss der fachlichen Fallprüfung von meiner Bußgeldstelle noch geprüft und bewertet werden.

14. Technik, Organisation

14.1 Neuaufstellung eines Kundenportals im Web nach einer Schutzverletzung

Verantwortliche gemäß Art. 24 DS-GVO setzen häufig Auftragsverarbeiter nach Art. 28 DS-GVO für die teilweise oder vollständige Realisierung und den Betrieb von Verarbeitungstätigkeiten ein. Diesen Auftragsverarbeitern ist gemäß Art. 28 Abs. 3 Buchst. c) DS-GVO vertraglich die Ergreifung aller gemäß Art. 32 DS-GVO erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung aufzuerlegen. Solche vertraglichen Vereinbarungen entbinden den Verantwortlichen nicht davon, die Wirksamkeit der Maßnahmen regelmäßig gemäß Art. 32 Abs. 1 Buchst. d) DS-GVO i. V. m. Art. 28 Abs. 3 Buchst. c), f) und h) DS-GVO zu überprüfen, zu bewerten und zu evaluieren.

Zu Beginn des Berichtszeitraums erreichte mich eine Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO eines Unternehmens in Nordhessen. Einem Kunden des Unternehmens war es gelungen, im Web-basierten Kundenportal des Unternehmens unberechtigt die personenbezogenen Daten eines Dritten, d. h. eines anderen Kunden einzusehen.

Ursächlich für die unberechtigte Offenlegung der personenbezogenen Kundendaten war das mangelhafte Authentifizierungsverfahren im Kundenportal. Kunden wurden zur Anmeldung am Kundenportal postalisch entsprechende Zugangscodes übersandt. Der Aufbau eines solchen Zugangscodes richtete sich nach einem festen Muster. Kam es bei der Anmeldung an der Web-Oberfläche des Kundenportals zu einem Fehler, so ließ die zurückgelieferte Fehlermeldung in bestimmten Fällen einen Rückschluss auf einzelne Stellen des Zugangscodes zu. Im Ergebnis konnte für einen fehlerhaft eingegebenen Zugangscode die exakte Stelle ermittelt werden, die für eine erfolgreiche Anmeldung angepasst werden musste.

Im Rahmen der Meldung teilte das Unternehmen mit, dass das Verfahren zur Generierung solcher datenschutzrechtlich zu bemängelnden Zugangscodes angepasst wurde und die bereits versandten Zugangscodes unbrauchbar gemacht wurden. Ferner wurde in der Meldung mitgeteilt, dass aus Sicht des Unternehmens nur ein Kunde von der unberechtigten Offenlegung betroffen war.

Die ergriffenen Maßnahmen waren anscheinend geeignet, um die konkreten Verletzungen des Schutzes personenbezogener Daten zu beheben und eine zukünftige Wiederholung zu verhindern.

Technische Außenbetrachtung

Bei dem von der Meldung betroffenen Kundenportal handelte es sich um ein über das öffentliche Internet zugängliches, Web-basiertes IT-System. In solchen Fällen analysieren Mitarbeiter meiner IT-Abteilung regelmäßig betroffene IT-Systeme in Form einer Außenbetrachtung. Hierbei werden die jeweiligen Web-Oberflächen aufgerufen und die zurückgelieferten Informationen ausgewertet. Dies schließt z. B.

– den aufgezeichneten Netzwerkverkehr,
– Metadaten des Hypertext Transfer Protocol (HTTP) und
– den Hypertext Markup Language-Code (HTML) der zurückgelieferten Seiten ein.

In Abhängigkeit von den Ergebnissen werden bei Bedarf vertiefende Analysen vorgenommen. Im vorliegenden Fall wurden z. B. Fehlerseiten analysiert und eingebundene Ressourcen näher inspiziert. Ziel dieses Vorgehens ist es, einen Eindruck von der zugrundeliegenden IT-Landschaft, den in ihr eingesetzten IT-Systemen sowie von der konkreten Ausgestaltung des Web-Angebotes zu erlangen. Im vorliegenden Fall konnten u. a. zwei zentrale IT-Systeme identifiziert werden, bei denen Anzeichen für Mängel bei der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO bestanden.

Bei einem Web-Server konnte z. B. die Anzeige einer sogenannten Standard-Startseite bewirkt werden. Sie enthielt den Hinweis, dass eine derartige Seite i. d. R. nur angezeigt würde, wenn der entsprechende Web-Server nicht angemessen konfiguriert sei. Zudem wurde über

– das eingesetzte Betriebssystem,
– die dem Web-Server zugrundeliegende Software, inkl. Versionsnummer, und
– installierte Komponenten, ebenfalls inkl. Versionsnummern, informiert.

Derartige Informationen dürften etwaigen Angreifern relevante Anhaltspunkte liefern. Daher ist die Anzeige einer solchen Standard-Seite zwingend zu unterbinden und gehört zur gängigen Praxis bei der Konfiguration von Web-Servern.

Für einen Applikations-Server konnte die Anzeige einer standardisierten Fehler-Seite herbeigeführt werden. Diese enthielt u. a. Informationen zu einem eingesetzten Software-Framework, inkl. Versionsnummer. Diese

Informationen legten den Schluss nahe, dass als Grundlage des Applikations-Servers eine über zehn Jahre alte Software zum Einsatz kam. Diese wird vom Hersteller schon länger nicht mehr mit Sicherheits-Updates und -Patches versorgt. Eine solche Software kann, insbesondere im Kontext von über das öffentliche Internet zugänglichen IT-Systemen, nicht als Stand der Technik gemäß Art. 32 Abs. 1 DS-GVO angesehen werden.

Termin vor Ort

Die obigen sowie weitere Erkenntnisse der technischen Außenbetrachtung führten zu weiteren Fragen und deuteten darauf hin, dass die ergriffenen technischen und organisatorischen Maßnahmen nicht ausreichten, um gemäß Art. 32 Abs. 1 DS-GVO ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zur weiteren Aufklärung des Sachverhalts war eine Innenbetrachtung der zugrundeliegenden IT-Landschaft, der konstituierenden IT-Systeme sowie der zugehörigen technischen und organisatorischen Maßnahmen erforderlich. Hierzu fand ein Termin in den Geschäftsräumen des Verantwortlichen statt, zu dessen Vorbereitung meine Mitarbeiter umfassende, vom Verantwortlichen angeforderte Unterlagen auswerteten.

Im Termin wurden fachliche, technische und organisatorische Themen im Zusammenhang mit dem Kundenportal und allgemein hinsichtlich des umschließenden Datenschutzmanagements beim Verantwortlichen erörtert. Hierbei stellte sich hieraus, dass die im Rahmen der technischen Außenbetrachtung identifizierten IT-Systeme innerhalb der IT-Landschaft des Verantwortlichen betrieben wurden, dass sämtliche Software-seitigen Wartungstätigkeiten aber an einen Auftragsverarbeiter gemäß Art. 28 DS-GVO ausgelagert worden waren. Bei diesem Auftragsverarbeiter handelte es sich gleichzeitig um den Hersteller der dem Kundenportal zugrundeliegenden Software. Am Termin nahmen keine Vertreter des Auftragsverarbeiters teil, so dass Detailfragen zur Ausgestaltung der Systeme nicht beantwortet werden konnten.

Im Ergebnis bestätigten sich die Anzeichen aus der technischen Außenbetrachtung, die vorher bei mir durchgeführt wurde. Gleichzeitig konnten die organisatorischen Bedingungen, die ursächlich für die Situation waren, im Rahmen des Termins geklärt werden. Hier stellte sich heraus, dass der Verantwortliche keine ausreichenden Maßnahmen ergriffen hatte, um seine Verpflichtungen im Sinne des Art. 32 Abs. 1 Buchst. d) DS-GVO i. V. m. Art. 28 Abs. 3 Buchst. c), f) und h) DS-GVO zu erfüllen.

Der Termin in den Geschäftsräumen des Verantwortlichen verlief sehr kooperativ und produktiv. Im Nachgang des Termins wurde von meinen Mitarbeitern eine detaillierte Zusammenfassung meiner Feststellungen erstellt und dem Verantwortlichen zur Stellungnahme übersandt. Der Verantwortliche

verpflichtete sich zur Umsetzung diverser Maßnahmen, um die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO herzustellen und auf Dauer zu gewährleisten. Dies schloss eine umfassende und tiefgehende Überprüfung der betroffenen IT-Systeme unter Zuhilfenahme externer Unterstützung mit ein. Die Ergebnisse der technischen Außenbetrachtungen durch meine Mitarbeiter sind grundsätzlich nicht mit einer ganzheitlichen Sicherheitsüberprüfung gleichzusetzen. Ihr Ziel ist es, aus technischer Perspektive zu überprüfen, ob sich Anzeichen für eine nicht mit der DS-GVO konforme Verarbeitung personenbezogener Daten ergeben.

Fazit

Die Mitarbeiter der IT-Abteilung meines Hauses führen regelmäßig technische Außenbetrachtungen von IT-Systemen durch, z. B. im Zusammenhang mit Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO. Im vorliegenden Fall lieferte die technische Außenbetrachtung starke Anzeichen dafür, dass technische und organisatorische Maßnahmen des Verantwortlichen nicht ausreichten, um die Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DS-GVO sicherzustellen.

Bei den gewonnenen Erkenntnissen handelte es sich um Symptome, deren Ursachen im Rahmen eines Termins in den Geschäftsräumen des Verantwortlichen ermittelt wurden. Es stellte sich heraus, dass sowohl technische als auch organisatorische Ursachen vorlagen. Ein wesentliches Problem lag in der praktischen Ausgestaltung des Verhältnisses zu einem Auftragsverarbeiter begründet. Hier zeigte sich, welche hohe Bedeutung der Überprüfung des Auftragsverarbeiters durch den Verantwortlichen gemäß Art. 28 Abs. 3 Buchst. h) beizumessen ist, auch wenn der Auftragsverarbeiter gemäß Art. 28 Abs. 3 Buchst. c) vertraglich zur Ergreifung erforderlicher Maßnahmen gemäß Art. 32 DS-GVO verpflichtet ist.

Ich möchte die kooperative und produktive Zusammenarbeit mit dem Verantwortlichen im vorliegenden Fall hervorheben. Auf effektive und effiziente Weise war es möglich, das Datenschutzniveau beim Verantwortlichen signifikant zu erhöhen und Prozesse zu initiieren, die zukünftig eine weitere Verbesserung bewirken werden. Auch habe ich gern dem Wunsch des Verantwortlichen entsprochen, gemeinsam mit ihm den vorliegenden Fall auf einem Treffen seines Verbands darzustellen. Dies gab mir die willkommene Gelegenheit, Verantwortliche eines Fachverbands mit ähnlichen technischen Lösungen hinsichtlich notwendiger datenschutzrechtlicher Anforderungen, Bewertungen und Umsetzungen zu sensibilisieren.

Der Auftragsverarbeiter und Hersteller der dem Kundenportal zugrundeliegenden Software wurde vom Verantwortlichen eingebunden. Dies galt

in besonderem Maße in Bezug auf erforderliche Anpassungen an der eingesetzten Software. Die Software wird vom Hersteller auch bei anderen Kunden eingesetzt. Ich gehe in diesem Zusammenhang davon aus, dass die erforderlichen Anpassungen diesen ebenso zur Verfügung gestellt und bei diesen umgesetzt werden. Hier behalte ich mir vor, entsprechende Prüfungen bei weiteren hessischen Kunden durchzuführen.

14.2
Dezentrale Datenhaltung und die Rechte der Betroffenen

Eine dezentrale Verwaltung und Verarbeitung personenbezogener Daten kann erheblich zur Sicherstellung einer Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b DS-GVO und einer Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DS-GVO beitragen. Gleichzeitig ergeben sich jedoch aus einer dezentralen Datenhaltung Herausforderungen in Bezug auf die Gewährleistung von Betroffenenrechten gemäß Kapitel III DS-GVO. Hieraus resultiert u. a. die Notwendigkeit einer umfassenden und frühzeitigen Berücksichtigung des Datenschutzes bei der Konzeption und beim Design von IT-Systemen und -Landschaften im Sinne des Datenschutzes durch Technikgestaltung gemäß Art. 25 DS-GVO.

Im Berichtszeitraum führte ich eine Prüfung bei einem hessischen Unternehmen durch, das für seine Kundinnen und Kunden Produkte herstellt. Gegenstand der Prüfung war die Fragestellung, ob und ggf. in welcher Form (zentral oder dezentral) das Unternehmen personenbezogene Daten zu den von ihm produzierten Produkten verarbeitet. Dies war für mich Anlass, mich intensiver mit der Thematik der dezentralen Datenhaltung in Bezug auf die Rechte der Betroffenen auseinanderzusetzen.

Die verteilte Datenhaltung

Den Ausgangspunkt zur Herstellung eines Produktes bildet meist ein Kaufvertrag, in dessen Kontext u. a. die Spezifika des konkreten Produktes festgehalten werden. Die entsprechenden personenbezogenen Daten werden hierzu in Form eines Auftrags in einem dafür vorgesehenen System zur Auftragsabwicklung gespeichert und zur weiteren Verarbeitung vorgehalten. Im Anschluss erfolgt die Produktion, an deren Ende die Auslieferung der Produkte an die Kundin oder den Kunden steht. Bereits im Zusammenhang mit der Produktion und der Auslieferung von kundenspezifischen Produkten werden personenbezogene Daten an weitere Systeme übertragen, z. B. Produktionsplanungs- und Steuerungssysteme. Im Rahmen der Auslieferung werden personenbezogene Daten dann an Logistik-Dienstleister übermittelt, die als Auftragsverarbeiter gemäß Art. 28 DS-GVO agieren. Nachdem ein

Produkt an eine Kundin oder einen Kunden übergeben wurde, wird es von Seiten des Herstellers weiterhin begleitet, u. a. im Rahmen der Produktbeobachtung und -verbesserung sowie von Garantie und Service.

Im Laufe des Lebenszyklus eines kundenspezifischen Produkts werden durch den Hersteller personenbezogene Daten zu unterschiedlichen Zwecken erhoben und verarbeitet. Bedingt durch die lange Nutzungsdauer der Produkte und die mit dieser in der Regel einhergehende Kundenbeziehung kommt im Laufe der Zeit eine größere Menge an personenbezogenen Daten zusammen.

Der Hersteller hat sich im vorliegenden Fall für eine weitgehend dezentrale Datenhaltung in Bezug auf personenbezogene Daten entschieden. Hierbei werden die für die jeweiligen Zwecke relevanten personenbezogenen Daten auf die zweckspezifischen IT-Systeme verteilt sowie in diesen vorgehalten und verarbeitet.

Jedes der IT-Systeme benötigt als Ausgangspunkt personenbezogene Basisdaten in unterschiedlichem Umfang, abhängig vom jeweiligen Einsatzzweck. Diese Daten werden in der Regel aus dem oben erwähnten System zur Auftragsabwicklung bezogen.

Im Laufe des Lebenszyklus eines kundenspezifischen Produkts kommt es zu unterschiedlichen Ereignissen, bei denen personenbezogene Daten erhoben werden. Beispiele hierfür sind Service-Kontakte, Reparaturen oder die Abwicklung von Garantiefällen. Je nach Relevanz der Daten für die jeweiligen Einsatzzwecke und dem Vorliegen einer entsprechend erforderlichen Rechtsgrundlage erfolgt eine Verteilung auf die IT-Systeme des Herstellers. Die Löschung der personenbezogenen Daten erfolgt ebenfalls auf Ebene der einzelnen IT-Systeme. Hierbei werden jeweils individuell anzuwendende Löschfristen berücksichtigt.

Die Rechte der betroffenen Personen

Zur Erfüllung der Informations- und Mitteilungspflichten des Verantwortlichen sowie zur Ausübung der Rechte durch betroffene Personen nach DS-GVO sind vom Verantwortlichen die Voraussetzungen zu schaffen und entsprechende Maßnahmen vorzusehen, die die Spezifika einer dezentralen Datenhaltung berücksichtigen.

Unter der Voraussetzung, dass der zugrundeliegende Prozess der Verteilung erhobener personenbezogener Daten über einen längeren Zeitraum unverändert bleibt, ergibt sich die Möglichkeit, die nachfolgend beschriebenen Schritte einmalig durchzuführen. Anschließend können die ermittelten Informationen im Rahmen der Erhebung weiterer personenbezogener Daten wiederholt bereitgestellt werden. In Fällen relevanter Änderungen

des Prozesses müssen diese Änderungen jedoch durch Anpassungen der bereitgestellten Informationen entsprechend reflektiert werden.

Die Informationspflichten gemäß der Art. 13 und 14 DS-GVO müssen bereits bei der Erhebung personenbezogener Daten erfüllt werden. Bereits zu diesem Zeitpunkt müssen Verteilung und Zwecke der Verarbeitung der Daten feststehen. Hierzu sind die einzelnen Zielsysteme zu identifizieren sowie jeweils die verarbeitungserheblichen Informationen zu ermitteln und aufzubereiten. Abschließend ist eine Zusammenführung der Einzelinformationen erforderlich.

Zur Gewährung des Auskunftsrechts gemäß Art. 15 DS-GVO ist bei einer verteilten Datenhaltung ein Prozess zur Identifikation derjenigen IT-Systeme zu implementieren, die personenbezogene Daten zur betroffenen Person verarbeiten. Im Rahmen dieses Prozesses müssen für die identifizierten IT-Systeme jeweils alle gemäß Art. 15 DS-GVO erforderlichen Informationen zurückgeliefert werden. Auf Basis dieser Informationen ist im Anschluss eine umfassende Auskunft zusammenzustellen und zu erteilen.

Zu Gewährung des Rechts auf Berichtigung gemäß Art. 16 DS-GVO, des Rechts auf Löschung gemäß Art. 17 DS-GVO und des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO sind mittels entsprechender Prozesse die jeweils betroffenen IT-Systeme zu identifizieren. Für jedes dieser IT-Systeme sind im Anschluss die zur Gewährung des jeweiligen Rechts erforderlichen Schritte durchzuführen. Hierbei sind die gemäß Art. 19 DS-GVO erforderlichen Mitteilungspflichten umzusetzen.

Zur Realisierung des Rechts auf Datenübertragbarkeit gemäß Art. 20 DS-GVO ist hinsichtlich der Ermittlung der relevanten Informationen analog zu Art. 15 DS-GVO vorzugehen. Das heißt, die gemäß Art. 20 Abs. 1 DS-GVO geforderte Zusammenstellung und Aufbereitung der personenbezogenen Daten sowie deren etwaige direkte Übermittlung zwischen Verantwortlichen gemäß Art. 20 Abs. 2 DS-GVO sind technisch zu implementieren.

Auch das Recht auf Widerspruch gemäß Art. 21 DS-GVO ist analog zu den Artikeln 16 bis 18 DS-GVO umzusetzen.

Möglichkeiten der Umsetzung

Die konkrete Umsetzung der in dem vorangegangenen Kapitel dargestellten Rechte der betroffenen Person muss in Form von entsprechenden datenschutzrechtlichen Begleitprozessen erfolgen. Zur Ausgestaltung derartiger Prozesse haben Verantwortliche unterschiedliche Möglichkeiten. Ein wesentliches Merkmal einer konkreten Umsetzung ist der Grad der Automatisierung.

Bei einer automatisierten und weitgehend technischen Umsetzung des Auskunftsrechts gemäß Art. 15 DS-GVO könnte ein IT-gestützter Prozess bspw.

alle potenziell betroffenen IT-Systeme kontaktieren. Aus diesen könnten dann alle für ein konkretes Auskunftsersuchen relevanten Informationen abgerufen werden. Die Aufbereitung der ermittelten Informationen könnte im Anschluss ebenfalls automatisiert erfolgen. Gleiches gilt für den anschließenden Versand.

Eine manuelle und hauptsächlich organisatorische Umsetzung eines Auskunfts-Prozesses müsste sich an der Organisationsstruktur des Verantwortlichen sowie der Zuordnung von Verarbeitungstätigkeiten und IT-Systemen zu Organisationseinheiten orientieren. Im Falle eines Auskunftsersuchens nach Art. 15 DS-GVO müssten alle Organisationseinheiten kontaktiert werden, in deren Kontext potenziell personenbezogene Daten zur betroffenen Person verarbeitet werden. Die Organisationseinheiten müssen sodann manuell ermitteln, ob sie tatsächlich entsprechende personenbezogene Daten verarbeiten. Für diesen Fall müssten sie alle zur Erteilung der Auskunft relevanten Informationen zusammenstellen und zurückmelden. Abschließend müssten die zurückgemeldeten Informationen zusammengeführt und der betroffenen Person übermittelt werden.

Bei der Ausgestaltung der datenschutzrechtlichen Begleitprozesse müssen Verantwortliche immer auch sonstige Rahmenbedingungen berücksichtigen, z. B. einzuhaltende Fristen oder verfügbare Mechanismen zur Ermittlung der Identität von betroffenen Personen. Die beiden obigen Beispiele stellen zwei entgegengesetzte Extreme hinsichtlich des Grades der Automatisierung für die Umsetzung datenschutzrechtlicher Begleitprozesse dar. In der Praxis dürften sich die tatsächlichen Implementierungen dazwischen bewegen.

So auch in dem von mir geprüften Fall. Wie viele andere Verantwortliche auch hatte der Verantwortliche wesentliche Teile seiner IT-Landschaft bereits vor dem Inkrafttreten der DS-GVO im Einsatz. Hieraus folgte, dass die konkreten Anforderungen aus dem Bereich der Rechte der betroffenen Personen gemäß Kapitel III DS-GVO bei der Umsetzung der Verarbeitungstätigkeiten und der zugehörigen IT-Systeme noch nicht berücksichtigt werden konnten. Dementsprechend waren die oben angeführten datenschutzrechtlichen Begleitprozesse zum großen Teil manueller Natur und mittels organisatorischer Maßnahmen umgesetzt. Hieraus resultierten, neben den vergleichsweise hohen Aufwänden zur manuellen Umsetzung der Prozesse, auch Herausforderungen in Bezug auf die Wahrung der zugehörigen Fristen.

Der Einfluss der Technikgestaltung

Art. 25 DS-GVO fordert einen Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. In Art. 25 Abs. 1 DS-GVO wird hierzu konkretisiert, dass der Verantwortliche sowohl zum Zeitpunkt der Festlegung als auch zum Zeitpunkt der Verarbeitung geeignete technische

und organisatorischen Maßnahmen trifft, um u. a. die Rechte der betroffenen Personen zu schützen.

Grundsätzlich fordert die DS-GVO von Verantwortlichen nicht, zur Wahrung der Rechte der betroffenen Personen vollautomatisierte datenschutzrechtliche Begleitprozesse umzusetzen. Dies gilt insbesondere vor dem Hintergrund, dass der Verantwortliche gemäß Art. 25 Abs. 1 DS-GVO bei der Ausgestaltung der Maßnahmen, und somit auch der datenschutzrechtlichen Begleitprozesse, den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und den Zweck der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für Rechte und Freiheiten der betroffenen Personen berücksichtigen muss.

Gerade in komplexen und über einen längeren Zeitraum hinweg fortentwickelten IT-Landschaften dürfte die nachträgliche Realisierung vollautomatisierter datenschutzrechtlichen Begleitprozesse mit erheblichen Implementierungskosten verbunden sein. Auf der anderen Seite dürfte die Durchführung vorwiegend organisatorisch umgesetzter datenschutzrechtliche Begleitprozesse in jedem Einzelfall im Vergleich zu vollautomatisierten Prozessen zu hohen Aufwänden führen. Beide Aspekte sollten bei der konkreten Ausgestaltung der datenschutzrechtlichen Begleitprozesse berücksichtigt werden. Hierbei spielen die konkreten Gegebenheiten im Einzelfall eine wesentliche Rolle, z. B. das Aufkommen an Anfragen gemäß Art. 15 DS-GVO sowie die Spezifika der IT-Landschaft und der konstituierenden IT-Systeme.

Es ist zu empfehlen, im Rahmen des Datenschutzmanagements eine Strategie für die Realisierung und Weiterentwicklung der datenschutzrechtlichen Begleitprozesse zu entwickeln und umzusetzen. Diese kann bspw. eine schrittweise Automatisierung vorsehen, die sowohl einzelne datenschutzrechtliche Begleitprozesse als auch einzelne IT-Systeme differenziert berücksichtigt. Die Abstimmung einer derartigen Strategie mit einem etwaig vorhandenen Enterprise Architecture Management, einer IT-Strategie sowie geplanten IT-Projekten sollte ebenfalls vorgenommen werden. So könnten bspw. Synergieeffekte genutzt werden, falls im Rahmen eines Anpassungs-Projekts für ein IT-System datenschutzrechtliche Begleitprozesse ebenfalls berücksichtigt werden. In Projekten zur Realisierung neuer Verarbeitungstätigkeiten und für die dazugehörigen IT-Systeme sollten datenschutzrechtlichen Begleitprozesse möglichst früh im Sinne des Datenschutzes durch Technikgestaltung berücksichtigt werden.

Für die Dauer des Bestehens eines datenschutzrechtlichen Begleitprozesses muss dieser regelmäßig überprüft werden. Dies gilt sowohl in Bezug auf das

technische als auch auf das organisatorische Umfeld des Prozesses sowie hinsichtlich der relevanten Verarbeitungstätigkeiten.

Fazit

Eine sinnvoll umgesetzte verteilte Datenhaltung und Verarbeitung personenbezogener Daten kann die Einhaltung der Grundsätze der Verarbeitung personenbezogenen Daten gemäß Art. 5 DS-GVO unterstützen. Dies gilt insbesondere für die Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b DS-GVO und die Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DS-GVO. Gleichzeitig ergeben sich hieraus spezifische Herausforderungen in Bezug auf die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO. Im Zusammenhang mit dem Datenschutz durch Technikgestaltung gemäß Art. 25 DS-GVO sind diese Herausforderungen entsprechend zu berücksichtigen. Bei einer frühzeitigen und umfassenden Berücksichtigung können in der Regel Synergieeffekte ausgeschöpft werden. Umgekehrt kann eine zu späte Berücksichtigung zu erheblichen und vermeidbaren Aufwänden führen. Eine regelmäßige Überprüfung datenschutzrechtlicher Begleitprozesse ist insbesondere in dynamischen Umgebungen unerlässlich.

14.3
Datenschutzrechtliche Anforderungen an Systemschnittstellen

In Verbindung mit mehreren Meldungen gemäß Art. 33 DS-GVO ist festzustellen, dass es häufig zu Verletzungen des Schutzes personenbezogener Daten durch Datenabflüsse an Systemgrenzen kommt. Das geschieht insbesondere, wenn Verantwortliche gemäß Art. 24 DS-GVO Verarbeitungstätigkeiten an Auftragsverarbeiter gemäß Art. 28 DS-GVO auslagern. Aus technischer Sicht empfiehlt sich eine bessere Überwachung der Funktionstüchtigkeit von Schnittstellen zwischen IT-Systemen und IT-Diensten zur Gewährleistung datenschutzrechtlicher Anforderungen gemäß Art. 32 DS-GVO auf Dauer. Mit Überwachung von Systemschnittstellen kann die Wahrscheinlichkeit des Eintritts von Verletzungen des Schutzes personenbezogener Daten reduziert werden, wenn hinsichtlich der Ergebnisse entsprechende Maßnahmen ergriffen werden.

Technisch realisierte Schnittstellen an Systemgrenzen zwischen IT-Systemen oder IT-Diensten sind auch Ausdruck der Vereinbarungen und Regelungen, die zwischen Verantwortlichen gemäß Art. 24 DS-GVO und Auftragsverarbeitern gemäß Art. 28 DS-GVO umgesetzt sind. Inhärente multilaterale Verbindungen zwischen eingesetzten IT-Systemen und IT-Diensten machen es aus technischer Sicht erforderlich, dass Systemgrenzen und Schnittstellen

besonders durch die Verantwortlichen zu überprüfen sind. Dabei sollte ein technisches Ziel sein, Datenflüsse auf allen Systemebenen zu kontrollieren. Denn jedes IT-System oder jeder IT-Dienst besitzt sowohl mindestens eine Systemgrenze als auch mindestens eine zur Nutzung bestimmte Schnittstelle. Nur über diese vorgesehenen Schnittstellen sollte auf bereitgestellte Funktionalitäten zugegriffen werden.

Eine unternehmens- oder organisationsinterne Überwachung sollte durch den Verantwortlichen gerade dann durchgeführt werden, wenn unternehmens- oder organisationsübergreifend IT-gestützte Prozesse implementiert werden. Implementierungen der jeweiligen IT-Systeme oder IT-Dienste müssen mit den genannten Vereinbarungen korrespondieren und die Zuständigkeiten eines Verantwortlichen bzgl. eines oder mehrerer Verarbeitungsvorgänge gemäß Art. 30 Abs.1 DS-GVO dargestellt werden. Nur wenn solche Vereinbarungen explizit und dokumentiert sind, können sie korrekt umgesetzt werden. Nach ihrer Bereitstellung ist die Überprüfung vereinbarungskonformer Verarbeitungen erforderlich. Ebensolche Zuständigkeiten sind im Zusammenhang mit den Zuständigkeiten eines Auftragsverarbeiters (Art. 30 Abs. 2 DS-GVO) zu sehen.

Aus technischer Sicht führt die Ausgestaltung des Verhältnisses zwischen Verantwortlichem zu seinem oder gar zu mehreren seiner Auftragsverarbeitern zur Realisierung einer multilateralen Datensicherheit. Einerseits bedeutet dies eine Trennung solcher Zuständigkeiten im Sinn klarer Festlegungen (Art. 30 DS-GVO). Anderseits ist zur Sicherstellung der Funktionstüchtigkeit der IT-Systeme und IT-Dienste unternehmens- bzw. organisationsübergreifend zu wirken. Um IT-gestützte Prozesse zu realisieren, sind IT-Systeme oder IT-Dienste in eine komplexe IT-Landschaft integriert. Die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO ist somit auch unternehmens- und organisationsübergreifend zu gewährleisten, insbesondere durch geeignete und angemessene technisch-organisatorische Maßnahmen.

Wenn ein Auftragsverarbeiter gleichzeitig Hersteller eingesetzter Software ist, hat er maßgeblichen Einfluss auf die Technikgestaltung im Sinne des Art. 25 DS-GVO. Aus dieser Konstellation ergeben sich spezielle Herausforderungen, eine multilaterale Datensicherheit zu realisieren bzw. eine geeignete und angemessene Überwachung durch den Verantwortlichen sicherzustellen. Mögliche Interessenskonflikte sollten vermieden werden.

Unternehmens- oder organisationsinterne Überwachungen von Systemgrenzen und ihrer Schnittstellen sind durch einen Verantwortlichen zu organisieren. Das bedeutet:

1. Die Überwachung von Systemgrenzen erfordert eine inhaltliche Betrachtung und entsprechende funktionale und nicht-funktionale Definitionen

von Schnittstellen, die den oben genannten datenschutzrechtlichen Anforderungen genügen müssen.

2. Gegen solche Schnittstellenspezifikationen ist die tatsächliche Implementierung und deren Einsatz in IT-Systemen und IT-Diensten regelmäßig zu prüfen, d. h. diese sind entsprechend eines vereinbarten Turnus durch den Verantwortlichen zu überwachen, und nicht nur beim Eintreten von Störungen oder gar Ausfällen zu inspizieren.
3. Im Rahmen dieser Überwachung muss die Wirksamkeit ergriffener technisch-organisatorischer Maßnahmen über Systemgrenzen hinweg nachgewiesen werden, um z. B. die Funktionstüchtigkeit systemübergreifender IT-gestützter Prozesse sicherzustellen.
4. Ergebnisse solcher Überwachungen sind datenschutzrechtlich zu bewerten.
5. Anhand dieser datenschutzrechtlichen Bewertung sollte der Verantwortliche, möglichst in Kooperation mit dem jeweiligen Auftragsverarbeiter, entscheiden, ob und wenn ja, welche Anpassungen und Verbesserungen auf welchen Ebenen vorzunehmen sind, so dass eine datenschutzkonforme Verarbeitung personenbezogener Daten unter Einsatz der IT-Systeme und IT-Dienste auf Dauer gewährleistet bleibt (Art. 32 DS-GVO). Somit sollten die Vereinbarungen bzw. datenschutzrechtlichen Anforderungen (Art. 24 DS-GVO i. V. m. 28 DS-GVO) erhalten bleiben.

Ferner können die Ergebnisse dieser regelmäßigen Überwachungen durch den Verantwortlichen auch zu einer datenschutzrechtlichen Neubewertung bestehender Vereinbarungen zur Auftragsverarbeitung oder ergriffener technisch-organisatorischer Maßnahmen führen, falls größere Abweichungen gegenüber der vorher bestimmten Schnittstellenspezifikation festgestellt werden.

Diese dargestellte Vorgehensweise scheint empfehlenswert, weil das Auftreten von Datenabflüssen durch unerwünschte Seiteneffekte an Systemschnittstellen zwischen IT-Systemen und IT-Diensten zu vermeiden ist, deren Funktionalitäten aus technischer Sicht verteilt realisiert sind. In Hinblick auf die eingegangenen Meldungen gemäß Art. 33 DS-GVO bestünde für Verantwortliche und Auftragsverarbeiter die Chance, solchen Datenabflüssen vorzubeugen. Des Weiteren kann davon ausgegangen werden, dass sich auch die Wahrscheinlichkeit reduziert, dass ein Verantwortlicher eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO zu melden hat.

14.4
Standard-Datenschutzmodell: Handbuch in Version 2.0

Das neue Handbuch 2.0 zum Standard-Datenschutzmodell (SDM-Handbuch) bietet Verantwortlichen und ihren Auftragsverarbeitern eine Anleitung, in welcher Weise datenschutzrechtliche Anforderungen in technische und organisatorische Maßnahmen umzusetzen sind.

Das SDM-Handbuch liegt in aktualisierter Version vor, (s. Web-Site des HBDI unter https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/SDM-Methode_V2.0a_0.pdf).

Der gesamte Text spricht Verantwortliche (Art. 24 DS-GVO) oder Auftragsverarbeiter (Art. 28 DS-GVO) direkt an. Das eröffnet diesen die Möglichkeit, das SDM zur Umsetzung von Betroffenenrechten auch in Kombination mit weiteren Vorgehensweisen zur Bewertung und Realisierung datenschutzrechtlicher Anforderungen mit, in und durch IT einzusetzen. Im 47. Tätigkeitsbericht habe ich bereits dargestellt, in welcher Weise Referenzmaßnahmen – sogenannte Bausteine – der Umsetzung von technisch-organisatorischen Maßnahmen (TOMs) dienen können und ebenso die datenschutzrechtliche Prüfpraxis im Allgemeinen unterstützt werden kann.

Die Version 2.0 ist im Vergleich zur vorausgegangenen Fassung neu gegliedert. Soweit die zu betrachtende Verarbeitung personenbezogener Daten rechtlich bewertet und grundsätzlich als zulässig erklärt wurde, wird im SDM-Handbuch das weitere Vorgehen für Verarbeitungstätigkeiten schrittweise dargestellt. Es umfasst die Teile A bis E.

Zweck des Standard-Datenschutzmodells (Teil A)

In Teil A wird das Vorgehensmodell mit dem Ziel dargelegt, geeignete und angemessene Maßnahmen zu ergreifen, so dass insbesondere Rechte und Freiheiten betroffener Personen (Art. 12 bis 15 DS-GVO) gewährleistet sind. Neben der datenschutzrechtlichen Einschätzung und Bewertung der gesetzlichen Grundlagen sind TOMs umsetzen. Hierbei ist eine Transformationsleistung zu erbringen, die entsprechende TOMs sowohl im Design eines Systems oder eines Dienstes (Art. 25 DS-GVO) einbezieht als auch ermöglicht, diese auf Dauer sicherzustellen (Art. 32 DS-GVO).

Interpretation von Begriffen mit technischem Bezug (Teil B)

Teil B liefert Interpretationen diverser Begriffe mit technischen Bezügen. Hierzu werden 23 solcher Begriffe erläutert, die in der DS-GVO Anwendung finden, wie Identifizierung, Authentifizierung, Wiederherstellbarkeit oder

Behebung und Abmilderung von Datenschutzverletzungen. Die hier vorgenommene Auswahl der in der DS-GVO verwendeten Begriffe verdeutlicht das unterschiedliche Abstraktionsniveau der zu behandelnden technischen Anforderungen. Daher sollte die Auswahl und die Umsetzung von TOMs in Bezug auf eine konkrete Verarbeitungstätigkeit einer genaueren technischen Betrachtung unter Anwendung von Teil C unterliegen.

Anwendung der Gewährleistungsziele nach DS-GVO (Teil C)

Teil C enthält eine Subsumtion der ausgewählten 23 Begriffe mit technischem Bezug unter die bekannten Gewährleistungsziele, die sich ebenso in Art. 5, Art. 25 oder Art. 32 DS-GVO finden lassen. Diese Gewährleistungsziele umfassen Festlegungen zur Datenminimierung, Vertraulichkeit, Integrität und Verfügbarkeit. Des Weiteren sind die Gewährleistungsziele der Nichtverkettung, der Transparenz und der Intervenierbarkeit eingeführt. Teil C schließt in Abschnitt C2 des SDM-Handbuchs mit einer Tabelle, die eine Zuordnung von Artikeln der DS-GVO zu Gewährleistungszielen enthält. Sie sind hinsichtlich der Umsetzung datenschutzrechtlicher Anforderungen richtungsweisend, ohne die Gestaltungsmöglichkeiten und Freiheitsgrade der tatsächlich auf Dauer eingesetzten IT einzuschränken.

Praktische Umsetzung (Teil D)

Teil D zielt auf die praktische Umsetzung. Konkretisierungen sind in Form von generischen Maßnahmen dargestellt, die auf gängige Ansätze in der IT verweisen (D1). Diese Form der Beschreibung ermöglicht es, typische Maßnahmen je Gewährleistungsziel technikneutral darzustellen. Es wird weiterhin erläutert, in welcher Weise das Verzeichnis der Verarbeitungstätigkeiten der Dokumentation, dem Nachweis und der eigenen Kontrolle beim Verantwortlichen und beim Auftragsverarbeiter bezüglich der ergriffenen TOMs dienen kann (D2). Teil D3 enthält eine neue Betrachtung zu Risiken und zum Schutzbedarf, die sowohl das entsprechende DSK-Kurzpapier als auch das „Working Paper 248“ (Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) abrufbar unter der Web-Site der Art. 29-Gruppe (heute: Europäischer Datenschutzausschuss, EDSA), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236) berücksichtigt. Grundzüge eines Datenschutzmanagements (DSM), wie im 47. Tätigkeitsbericht dargestellt, sind jetzt in Abschnitt D4 aufgenommen. Des Weiteren werden Zusammenhänge wie Planung und Spezifikation, Implementierung, Kontrollen und Überprüfungen der auf Dauer betriebenen IT dargestellt, die Evaluationsergebnisse liefern und mittels des Verzeichnisses der Verarbeitungstätigkeiten genutzt werden können. Hiermit erhalten Verantwortliche und Auftragsverarbeiter ein

Konzept für einen DSM-Zyklus, der auch ihre Zusammenarbeit organisieren kann, so dass schließlich die zu den Verarbeitungsvorgängen gehörenden technisch-organisatorischen Maßnahmen für Systeme und Dienste auf Dauer gewährleistet sind (Art. 24, Art. 28, Art. 30 und Art. 32 DS-GVO).

Organisatorische Rahmenbedingungen (Teil E)

In Teil E werden organisatorische Rahmenbedingungen dargestellt. Dazu gehört das Zusammenwirken von SDM und BSI-Grundschutz. Es wird ein Einblick gegeben, in welcher Weise das Standard-Datenschutzmodell entwickelt wurde und weiterentwickelt werden soll.

Fazit

Mit der Anwendung des SDM-Handbuches 2.0 erhalten Verantwortliche und Auftragsverarbeiter eine sehr weitgehende Unterstützung, die Rechte betroffener Personen mit der Auswahl geeigneter und angemessener TOMs nach den Vorgaben der DS-GVO zu wahren.

14.5 Leitlinie des Europäischen Datenschutzausschusses zum Thema Blockchain

Aktuell wird auch in der Öffentlichkeit über den Einsatz von Blockchain Technologien in sehr unterschiedlichen Einsatzgebieten, besonders auch als Kryptowährungen diskutiert. Regelungen zu dieser Technologie befinden sich in Arbeit.

Seit Juni 2019 hat der Europäische Datenschutzausschuss (EDSA) der Expertengruppe Technologie[1] und Expertengruppe Finanzwesen[2] gemeinsam das Mandat zur Erarbeitung einer Leitlinie zum Thema Blockchain erteilt. Unter der Federführung Frankreichs wird aktuell diese Leitlinie bzgl. der verschiedenen Einsatzmöglichkeiten von Blockchains als Distributed Ledger Technologie[3] erarbeitet. Eine Mitarbeiterin aus meiner IT-Abteilung arbeitet an der Erstellung mit. Weitere Berichterstatter kommen aus Italien, Lichtenstein und Spanien, und auch ein Vertreter des Europäischen Datenschutzbeauftragten ist beteiligt.

---

1 Expertgroup Technology of the European Data Protection Board

2 Expertgroup Finanical Matters of the European Data Protection Board

3 In ihrem Ursprung als verteilte Register eingesetzte Technologie und heutiger Anwendungsgebiete.

Technische Einblicke

Aus zunächst technischer Perspektive werden in dieser Leitlinie die technischen Voraussetzungen erörtert. Hierzu werden Grundlagen und unterschiedliche Formen von Blockchains erklärt. Die Basis einer jeden Blockchain ist eine verkettete Folge von i. d. R. gleichartigen Blöcken, die über die gesamte Lebensdauer fortgeschrieben werden. Jede beteiligte Stelle speichert ihre eigene Kopie dieser Kette mit allen Blöcken. Über einen Konsensmechanismus wird sichergestellt, dass bei allen Beteiligten die identische Kette entsteht.

Die Struktur einer Blockchain kann öffentlich oder nicht-öffentlich sein. Aus der Sicht der Informationstechnik liegt der Unterschied zunächst in den Möglichkeiten, wer, unter welchen Umständen, die Struktur der Blockchain selbst kopieren und fortschreiben kann, d. h. in welcher Weise der Konsensmechanismus eben diesen herstellt. Somit ist je nach Einsatzgebiet und Anwendungskontext zu erörtern,

– durch wen die Blockchain fortgeschrieben werden kann und
– wer die in der Blockchain gespeicherten Daten einsehen darf oder nicht; d. h. sollen die Daten frei verfügbar und somit transparent oder sollen sie vertraulich sein.

Hieraus resultiert z. B. die Frage, ob eine Stelle, die eine solche Blockchain fortschreiben kann, auch im Sinne der DS-GVO verantwortlich ist. Aus datenschutzrechtlicher Sicht werden hinsichtlich der Beteiligten deren Verantwortung und Rollen diskutiert.

Des Weiteren ist zu berücksichtigen, an welchen Orten die Blockchain gespeichert ist. Daher ist bzgl. der Struktur einer Blockchain ihre Manipulationssicherheit sicherzustellen. Die Anwendung eines Konsensmechanismus muss sowohl sicherstellen, dass nur Beteiligte, die berechtigt sind, Blöcke in die Kette einfügen als auch die Möglichkeit der Manipulation ausschließen. Das wird über sogenannte Validatoren sichergestellt. Oftmals werden Validatoren durch das Lösen mathematischer Rätsel realisiert, womit verlangt ist, dass gleichzeitig alle bisher in der Kette befindlichen Blöcke überprüft werden. Wer also ein solches Rätsel lösen kann, der hat alle Blöcke überprüft und darf selbst einen Block einfügen. Nachdem ein Block eingefügt ist, kann dieser nicht mehr verändert werden, ansonsten würde das Prinzip des Rätsellösens untergraben werden. Umso länger die Kette in der Blockchain ist, desto rechenintensiver ist das Einfügen eines weiteren Blocks, da immer jeder Block in der Kette validiert werden muss. – In nicht-öffentlichen Blockchains gibt es inzwischen andere Konsensmechanismen, die eher auf einer Abstimmung z. B. mit Mehrheitsprinzip basieren. Sie sind somit weniger rechenzeitintensiv.

Selbstverständlich ist aus datenschutzrechtlicher Sicht ebenso eine Klassifizierung der Daten in den Blöcken wesentlich. Diesbezüglich ist

– zwischen Daten, die in Blöcken selbst gespeichert werden, ein sogenannter „pay load“, und
– Referenzen auf Daten zu unterscheiden, womit diese nicht innerhalb der Blockchain, sondern an einem anderen Speicherort liegen.

Wenn Daten als „pay load“ in den Blöcken einer Blockchain vertraulich zu behandeln sind, dann sind sie verschlüsselt zu speichern.

Offensichtlich ist, dass bei einer dezentralen, gar im Netz verteilten Struktur, wie der Blockchain, IT-Sicherheitsaspekte zu behandeln sind, die speziell auch auf den dauerhaften Betrieb einer Blockchain zielen.

Ausblick: Betrachtung von speziellen Anwendungen von Blockchains

Die entwickelten datenschutzrechtlichen Kriterien sollen beispielhaft auf spezielle Implementierungen von Blockchains angewendet werden. Dazu gehören selbstverständlich unterschiedliche Kryptowährungen, für die die Expertengruppe Finanzwesen eine entsprechende datenschutzrechtliche Bewertung vornehmen wird. Des Weiteren sollen bestimmte Register, wie Grundbücher, betrachtet werden. Ferner sind Optimierungen von Fabrikationsprozessen von Interesse, sofern personenbezogene Daten verarbeitet werden. Schließlich soll insbesondere die Verwaltung digitaler Identitäten angesehen und datenschutzrechtlich bewertet werden.

Fazit

Die technologisch weit fortgeschrittene Entwicklung von Blockchains und ihrer vielfältigen Einsatzgebiete macht eine datenschutzrechtliche Bewertung notwendig. Hier ist es zu begrüßen, dass durch das Mandat des EDSA mit einer technischen Betrachtung unter datenschutzrechtlichen Aspekten begonnen wurde.

15. Bußgeldverfahren, Datenschutzverletzungen gemäß Art. 33 DS-GVO

15.1
Bußgeldverfahren im Jahr 2019

Im Berichtsjahr waren von mir Bußgeldverfahren durchzuführen, bei denen es auch um Sachverhalte von Datenschutzverletzungen ging, die in der Praxis leider immer wieder auftreten. Im öffentlichen Bereich sind dies zweckwidrige Datenabrufe und/oder zweckwidrige Datenverwendungen durch Mitarbeiter oder Mitarbeiterinnen. Im nichtöffentlichen Bereich führt die Nichtbestellung von betrieblichen Datenschutzbeauftragten trotz Bestellpflicht zu Sanktionen.

1.
Bußgeld bei sogenanntem Mitarbeiterexzess im öffentlichen Bereich

Auch gegen Mitarbeiterinnen oder Mitarbeiter im öffentlichen Bereich können unter bestimmten Umständen Bußgelder verhängt werden.

Das mag auf den ersten Blick verwundern, denn Hessen hat sich gegen die Möglichkeit in Art. 83 Abs. 7 DS-GVO entschieden, gegen Behörden und öffentliche Stellen Bußgelder verhängen zu können. Es wurde vielmehr in § 36 Abs. 2 HDSIG explizit ein Ahndungsverbot aufgenommen, wonach wegen Verstößen gegen Art. 83 Abs. 4 bis 6 DS-GVO keine Geldbuße gegen Behörden und sonstige öffentliche Stellen verhängt werden.

Eine Ausnahme davon ist aber dann zu machen, wenn das schädigende Verhalten einer Mitarbeiterin oder Mitarbeiters dem öffentlichen Arbeitgeber nicht zuzurechnen ist. Wie die beiden nachfolgenden Beispiele zeigen, gibt es Formen des Mitarbeiterexzesses, die zu einem Bußgeld gegen Mitarbeiterinnen und Mitarbeitern im öffentlichen Dienst führen können.

Zweckwidriger Datenabruf im Ordnungsamt

In einem Fall hatte eine Mitarbeiterin eines Ordnungsamtes einer hessischen Stadt ohne dienstlichen Anlass eine elektronische Einwohnermeldeabfrage (Intranet-Auskunft) vorgenommen und Angaben zu den Daten einer bestimmten Person angefordert. Aufgrund einer eingetragenen Auskunftssperre nach § 51 Bundesmeldegesetz (BMG) wurde die Person darüber schriftlich informiert, dass diese Mitarbeiterin des Ordnungsamtes dieser Stadt ein Auskunftsersuchen gestellt hatte. Ein gleichlautendes Schreiben wurde auch an die Dienststelle des Ehemanns der Person versandt.

Die Kenntnis der abgefragten personenbezogenen Daten war zur Erfüllung der der Mitarbeiterin des Ordnungsamtes obliegenden Aufgaben nicht erforderlich. Eine Rechtsgrundlage für die Abfrage bestand nicht und es lag auch keine Einwilligung der betroffenen Person vor. Vielmehr wurden die durch diese Einwohnermeldeanfrage erlangten personenbezogenen Daten der betroffenen Person eigenmächtig zu einem anderen Zweck verarbeitet, als zu dem Zweck, zu welchem die Daten ursprünglich erhoben wurden, verwendet. Damit hat die Mitarbeiterin des Ordnungsamtes gegen das Zweckbindungsgebot des Art. 5 Abs. 1 lit. b DS-GVO verstoßen. Dennoch ist dieser Verstoß dem Ordnungsamt nicht zuzurechnen. Die Mitarbeiterin hat die Handlung zwar von ihrem Arbeitsplatz aus unter Einsatz der zur Verfügung stehenden Arbeitsmittel begangen, jedoch nicht in Ausübung ihrer beruflichen Tätigkeit, sondern ausschließlich privat. Die Mitarbeiterin ist auch nicht als eigene öffentliche Stelle im Sinne des § 2 HDSIG zu qualifizieren.

Der Verstoß wurde von mir gem. Art. 83 Abs. 5 lit. a DS-GVO i. V. m. Art. 5 Abs. 1 lit. b DS-GVO mit einem Bußgeld von 150 € geahndet. Bei der Zumessung wurde berücksichtigt, dass nur eine Person vom Sachverhalt betroffen war und bislang keine weiteren datenschutzrechtlichen Beanstandungen vorlagen. Bußgeldsenkend wurde berücksichtigt, dass der Fall im Zeitpunkt der Entscheidung bereits ein Jahr zurücklag. Zur Orientierung wurde das monatliche Nettoeinkommen hinzugezogen.

Zweckwidrige Verwendung dienstlich erlangter Daten

Im Rahmen einer Datenpannenmeldung durch den Polizeipräsidenten nach Art. 33 DS-GVO erhielt ich Nachricht darüber, dass ein Polizeibeamter vom Teil eines dienstlichen Dokuments, einer Strafanzeige, ein Foto fertigte, das in einem sog. Gruppen-Chat des Instant-Messanging-Dienstes WhatsApp eingestellt wurde. Die Aufnahme war mit einer Bemerkung versehen, aus der hervorging, dass es sich um eine Anzeige handelte, von wem diese stammte und aus welchem Anlass sie erstattet worden war. Teilnehmer des Gruppen-Chat waren bestimmte Personen eines Vereinsvorstandes. Sie alle erhielten das Foto mitsamt der Bemerkung.

Die zuständige Sachbearbeitung meines Aufsichtsbereichs gab diesen Fall an die Bußgeldstelle meiner Dienststelle ab. Diese eröffnete nach Prüfung ein Bußgeldverfahren. Darin wurde festgestellt, dass mit der Übermittlung eines Teils der Strafanzeige an die Mitglieder der Chat-Gruppe personenbezogene Daten zu einem anderen Zweck verarbeitet wurden, als zu dem die Daten ursprünglich erhoben wurden. Auch dieser Verstoß war der Polizeidienststelle nicht zuzurechnen. Die Handlung wurde zwar unter anderem unter Einsatz der dienstlich zur Verfügung stehenden Arbeitsmitteln begangen, jedoch nicht

in Ausübung der beruflichen Tätigkeit, sondern ausschließlich zu privaten Zwecken. Daher greift das Ahndungsverbot nach § 36 Abs. 2 HDSIG in diesem Fall nicht ein und es handelt sich nicht um ein der Dienststelle zurechenbares Verhalten. Der Mitarbeiter war auch nicht als eigene öffentliche Stelle im Sinne des HDSIG zu qualifizieren. Es wurde auf ein Bußgeld in Höhe von 500 € erkannt. Zu berücksichtigen war bei der Zumessung, dass es ein leichter Verstoß war, weil nur ein Auszug aus der Strafanzeige veröffentlicht wurde und nur eine Person betroffen war. Zugunsten des Betroffenen war zu berücksichtigen, dass bislang keine datenschutzrechtlichen Beanstandungen gegen ihn vorlagen. Deutlich bußgeldmildernd wirkte sich aus, dass der Vorfall vollständig eingeräumt wurde und der Betroffene sich für seine Tat entschuldigt hat. Zu Lasten des Betroffenen war zu berücksichtigen, dass er personenbezogene Daten mittels eines Instant-Messaging-Dienstes, der auf einfachem Weg eine Weiterleitung der Nachricht an einen großen Adressatenkreis ermöglicht, an mehrere Personen übermittelt hat. Berücksichtigt wurde zudem das monatliche Einkommen des Betroffenen.

2.
Bußgeld wegen Nichtbestellung eines betrieblichen Datenschutzbeauftragten

Auch die (irrtümliche) fehlende Bestellung eines betrieblichen Datenschutzbeauftragten führt immer wieder zu Maßnahmen meinerseits.

Ein noch nach altem Datenschutzrecht zu entscheidender Fall führte im Berichtsjahr zu einem Bußgeld in Höhe von 3.800,00 €. Auf den Fall wurde ich durch eine Beschwerde aufmerksam. Ein Unternehmen hatte entgegen der gesetzlichen Bestimmungen keinen internen Datenschutzbeauftragten bestellt. Meine Ermittlungen ergaben nach einem schleppenden Schriftverkehr, dass die Firma einen betrieblichen Datenschutzbeauftragten (bDSB) hätte bestellen müssen. Nach Fristsetzung meinerseits wurde zwar ein Datenschutzbeauftragter bestellt. Diese Bestellung war aber zu beanstanden, da es dem bDSB an der erforderlichen Sachkunde nach § 4f Abs. 2 BDSG a. F. fehlte und die Möglichkeit einer Interessenkollision bestand. Die bestellte Person war Geschäftsführer eines Tochterunternehmens der betroffenen Firma und damit als Entscheider nicht in ausreichendem Maße unabhängig.

Daraufhin wurde eine neue interne Datenschutzbeauftragte für das Unternehmen bestellt.

Da in der Zwischenzeit durch die Geltung der DS-GVO eine neue Rechtslage eingetreten war, war zunächst zu klären, ob die neuen Reglungen der DS-GVO einer Ahndung entgegenstehen. Das war nicht der Fall, auch nach Geltung

der DS-GVO und Inkrafttreten der Neufassung des BDSG am 25.05.2018 war die Nichtbestellung eines erforderlichen Datenschutzbeauftragten bußgeldbewehrt. Dabei war jedoch die Sanktionsregelung nach § 43 Abs. 1 Nr. 2 a. F. heranzuziehen, da diese gegenüber der neuen Regelung in Art. 83 Abs. 4 lit. a DS-GVO i. V. m. Art. 37 Abs. 4 S. 1 DS-GVO i. V. m. § 38 BDSG n. F. das mildere Gesetz i. S. v. § 4 Abs. 3 OWiG ist.

Für die Zumessung der Geldbuße war relevant, dass die fahrlässig begangene Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 2 BDSG a. F. nach § 43 Abs. 3 BDSG a. F. mit einer Geldbuße bis zu 50.000, 00 € bedroht war. Die objektive Bedeutung der Ordnungswidrigkeit war von durchschnittlicher Art, die Schwere der begangenen Zuwiderhandlung war aufgrund der erheblichen Dauer dagegen als überdurchschnittlich einzustufen. Verschärfend wurde berücksichtigt, dass dem Unternehmen durch die Nichtbestellung ein deutlicher wirtschaftlicher Vorteil zugeflossen ist. Es sind Kosten über mehr als sieben Jahre erspart worden. Bußgeldmindernd wurde wiederum die überlange Verfahrensdauer und die (nur) fahrlässige Begehung berücksichtigt.

Eine weitere, in der Praxis häufig vorkommende Fallgestaltung, die zu einem Bußgeld führen kann, ist die Verletzung der Meldepflicht bei Vorliegen einer Datenpanne nach Art. 33 DS-GVO. Ein Beispielsfall ist unter Ziff. 15.3 dargestellt.

15.2
Bußgeldzumessung durch die Aufsicht

Am 16. Oktober 2019 hat die DSK das Konzept zur Zumessung von Bußgeldern nach der DS-GVO der Öffentlichkeit vorgestellt. Bislang gab es für Informationen zu Art. 83 Abs. 1 und 2 DS-GVO eine Leitlinie (Workingpaper wp253), die sich mit der Auslegung von Art. 83 DS-GVO befasst und so eine europaweit einheitliche Auslegung der Norm sicherstellen soll, sowie das Kurzpapier Nr. 2 „Aufsichtsbefugnisse und Sanktionen“ der Datenschutzkonferenz (DSK). Dieser Beitrag befasst sich mit dem aktuellen Sachstand zur Bußgeldzumessung.

Auf dem Weg zum Bußgeldkonzept

Das Dokument wp253 war bereits Gegenstand des 46. TB (siehe dort Ziff. 2.2.2). Es befasst sich im Wesentlichen mit der Frage der Entscheidung der Aufsichtsbehörde, *ob* ein Bußgeld verhängt werden soll. Damit wurden aber die Anforderungen aus Art. 70 lit. k) DS-GVO nach weiteren Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Absätze 1, 2, und 3 DS-GVO und die Festsetzung von Geldbußen, insbeson-

dere deren Höhe, noch nicht umgesetzt. Aber es waren die richtigen Schritte in die richtige Richtung getan. Die Artikel 29-Gruppe hatte, wie schon im 46. TB berichtet, in der Novembersitzung 2017 aus der Enforcement Subgroup eine permanente Taskforce, die Taskforce Fining, eingerichtet. Zu deren Hauptaufgaben zählt die Harmonisierung der Berechnung von Geldbußen (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610112). Seit ihrem ersten Meeting im Dezember 2017 befasst sich die Taskforce mit der Harmonisierung der teilweise erheblich unterschiedlichen Praktiken in den Mitgliedstaaten und diskutiert darüber, wie es weitergehen soll.

Einen gemeinsamen europaweiten Rahmen für die Festsetzung von Geldbußen gibt es bislang nicht. Vielmehr haben die Mitgliedstaaten vereinzelt für die Übergangszeit nationale Ansätze entwickelt. So haben die Niederlande im Amtsblatt Nr. 14586 vom 14. März 2019 Richtlinien der Behörde für personenbezogene Daten vom 19. Februar 2019 zur Festlegung der Höhe der Bußgelder (Bußgeldrichtlinien der Behörde für personenbezogene Daten 2019) veröffentlicht. In Deutschland hat sich die DSK mit der Frage der Harmonisierung der Bußgeldzumessung auf nationaler Ebene befasst und ein erstes Konzept zur Bußgeldzumessung bei Verstößen gegen die DS-GVO unter Orientierung an den Modellen aus dem nationalen Kartellrecht und Wertpapier- und Aktienrecht erarbeitet. Das Bußgeldkonzept der DSK war unter TOP 16 Thema auf der 2. Zwischenkonferenz im Juni 2019 (Protokoll: https://www.datenschutzkonferenz-online.de/media/pr/20190622_pr_mainz.pdf). Die DSK begrüßte mehrheitlich das Konzept als geeignete Grundlage für die Zumessung von Bußgeldern und bat den AK Sanktionen, das Konzept unter Einbeziehung der damit gemachten praktischen Erfahrungen der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder weiterzuentwickeln (16 Zustimmung, 1 Enthaltung, 0 Ablehnung).

Auf der 3. Zwischenkonferenz der DSK am 12.9.2019 in Mainz befasste sich die DSK mit der Frage der Veröffentlichung des Bußgeldkonzepts der Datenschutzkonferenz. Anlass waren vermehrt auftretende Anfragen auf Übersendung des von der Konferenz erstellten Entwurfs eines Bußgeldkonzeptes aus dem Juni 2019 (Protokoll: https://www.datenschutzkonferenz-online.de/media/pr/20191126_protokoll_3_zwiko_2019.pdf).

Die DSK sah sich veranlasst, das Konzept zur Zumessung von Geldbußen in Verfahren gegen Unternehmen vorzustellen. Es ist im Anhang I Ziff. 3.1 abgedruckt und steht im Internet auf Deutsch unter https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf bzw. in Englisch unter https://www.datenschutzkonferenz-online.de/media/pm/20191126_dsk_fining_concept_en.pdf zur Verfügung. Eine förmliche

Entschließung oder ein Beschluss der DSK liegen bislang nicht vor, so dass das Konzept aus meiner Sicht nicht verbindlich ist.

Das veröffentlichte Bußgeldkonzept

Das Konzept betrifft ausschließlich die Bußgeldzumessung in Verfahren gegen Unternehmen im Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) auf dem Gebiet der Bundesrepublik Deutschland. Das Konzept ist auch weder für grenzüberschreitende Fälle noch für andere Datenschutzaufsichtsbehörden der EU bindend. Es findet insbesondere keine Anwendung auf Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit. Ferner entfaltet es keine Bindung hinsichtlich der Festlegung von Geldbußen durch Gerichte.

Die DSK kann jederzeit eine Aufhebung, Änderung oder Erweiterung ihres Konzepts mit Wirkung für die Zukunft beschließen. Das Konzept verliert seine Gültigkeit, sobald der EDSA seine abschließenden Leitlinien zur Methodik der Festsetzung von Geldbußen erlassen hat.

Die Bußgeldzumessung nach dem Konzept orientiert sich am Umsatz der Unternehmen. Die DSK ist der Auffassung, dass in einem modernen Unternehmenssanktionsrecht mit erheblichen maximalen Bußgeldbeträgen, das sich zugleich an eine Vielfalt unterschiedlich großer Unternehmen richtet, der Umsatz eines Unternehmens eine geeignete, sachgerechte und faire Anknüpfung zur Sicherstellung der Wirksamkeit, Verhältnismäßigkeit und Abschreckung darstellt.

Die Bußgeldzumessung in Verfahren gegen Unternehmen erfolgt in fünf Schritten (siehe Bußgeldkonzept im Anhang I 3.1):

Schritt 1: Zunächst wird das betroffene Unternehmen mittels seines Umsatzes einer Größenklasse zugeordnet,

Schritt 2: danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt,

Schritt 3: dann wird ein wirtschaftlicher Grundwert ermittelt,

Schritt 4: dieser Grundwert wird mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert und

Schritt 5: abschließend wird der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst.

Nach Auffassung der DSK garantiert das Verfahren eine nachvollziehbare, transparente und einzelfallgerechte Form der Bußgeldzumessung. Soweit die Schritte 4 und 5 bisweilen von Unternehmensvertretern für zu undurchschaubar befunden wurden, ist festzustellen, dass es nicht Sinn des Konzeptes ist,

das Bußgeld vorab zu kalkulieren. Die Schritte 4 und 5 tragen Art. 82 Abs. 1 und 2 DS-GVO Rechnung.

Entschließung der DSK zur Zurechnung

Dem Bußgeldkonzept der DSK ging ein wichtiger Schritt zur Harmonisierung der Bebußung nach DS-GVO voraus. In der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019 fasste die DSK die Entschließung „Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!“ (s. a. Anhang I 1.1).

Hintergrund war, dass die alten nationalen Haftungsregeln bisher nicht europarechtskonform der neuen Rechtslage angepasst wurden. § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) verweist auf zurechnungseinschränkende Regelungen im OWiG. Das nationale Recht mit dem zugrundeliegenden Rechtsträgerprinzip kollidiert mit europäischen Anforderungen und auch Traditionen. Unternehmen haften im Rahmen von Art. 83 DS-GVO für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Diese Haftung für Mitarbeiterverschulden ergibt sich vielmehr aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt nach der Definition des EuGH, dass ein Unternehmen „jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung“, ist (EuGH in ständiger Rechtsprechung seit Rs. C-41/90 (Höfner und Elser), Slg. 1991, I-1979, Rn. 21). Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse“), sind ausgenommen.

Mit dieser Entschließung ist die Praxis der DSK vorerst vorbehaltlich einer abweichenden Gerichtsentscheidung geklärt. Die DSK hatte bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz den Gesetzgeber darauf aufmerksam gemacht, dass diese Bestimmungen

den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen. Im Ergebnis aber bislang ohne Erfolg.

Es bleibt abzuwarten, inwieweit die Vereinbarungen aus dem Koalitionsvertrag der Regierungsparteien auf Bundesebene zu einer Modernisierung des Unternehmenssanktionsrechts führen. Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

15.3
Bußgeld nach Verletzung der 72-Stunden-Frist bei einer Meldung nach Art. 33 DS-GVO durch eine Reha-Klinik

Die Begründung für die verspätete Meldung nach Art. 33 Abs. 1 DS-GVO muss umso tragfähiger sein, je gravierender die Datenschutzverletzung ist und je länger die 72-Stunden-Frist überzogen wird. Die Angabe, die Mitarbeiter hätten die Pflicht zur Meldung nicht gekannt, reicht als Begründung in der Regel nicht aus.

Ausgangsfall

Ende des Jahres 2018 wurde mir von einer Reha-Klinik eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 Abs. 1 DS-GVO gemeldet. Hierbei ging es darum, dass ein Entlassungsbericht eines Patienten und damit Gesundheitsdaten an einen anderen Patienten übermittelt wurden. Der Patient, der den falschen Brief postalisch erhalten hatte, informierte die Klinik telefonisch an einem Freitag über den Vorfall. Die Meldung nach Art. 33 Abs. 1 DS-GVO an meine Behörde durch die Klinik erfolgte erst sieben Tage später. Als Begründung für die verspätete Meldung des Vorfalls gab die Klinik zum einen an, dass ein Wochenende dazwischen lag. Zum anderen sei ein derartiger Fehler in der Klinik noch nicht vorgekommen, weshalb es zu Versäumnissen bei der Weitergabe von Informationen seitens der beteiligten Mitarbeiter gekommen war.

Rechtliche Bewertung

Die zu späte Meldung stellte hier einen Verstoß gegen Art. 33 Abs. 1 DS-GVO dar. Zwar hat die Klinik die verspätete Meldung begründet, die Begründung war aus meiner Sicht jedoch unzureichend.

Der DS-GVO sind keine Anhaltspunkte über die Qualität der Begründung zu entnehmen. Es ist jedoch davon auszugehen, dass sie umso tragfähiger sein muss, je gravierender die Datenschutzverletzung ist und je länger die

72-Stunden-Frist überzogen wird (*Jandt* in: Kühling/Buchner, DS-GVO, Art. 33 Rn. 16, 2. Aufl. 2018).

In Hinblick darauf, dass hier ein Entlassungsbericht und damit Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO einer unbefugten Person bekannt geworden sind und dass zwischen dem Bekanntwerden des Vorfalls und der Meldung eine Woche vergangen war, waren an die Begründung höhere Anforderungen zu stellen. Der Klinik war hier insbesondere anzulasten, dass sie ihre Mitarbeiter trotz der Geltung der DS-GVO seit dem 25.05.2018 immer noch nicht ausreichend über ihre Pflichten unterrichtet hatte.

Wegen des Verstoßes gegen Art. 33 Abs. 1 DS-GVO habe ich den Fall an meine Bußgeldstelle zur Prüfung der Verhängung eines Bußgeldes nach Art. 83 DS-GVO gegeben. Das Bußgeldverfahren mündete in einen Bußgeldbescheid, mit dem ein Bußgeld in Höhe von 6.800 € festgesetzt wurde. Das Bußgeld liegt deutlich im unteren Bereich des Bußgeldrahmens, da verschiedenen Faktoren i. S. d. Art. 83 Abs. 2 DS-GVO bußgeldmindernd berücksichtigt werden konnten. Neben anderen Faktoren wurde berücksichtigt, dass es eine fahrlässige Tatbegehung war, dass der Sachverhalt vollumfänglich eingeräumt wurde, dass Maßnahmen ergriffen wurden, um der Datenschutzverletzung abzuhelfen, sowie zeitnahe und unaufgeforderte Entschuldigung beim Patienten.

Empfehlung

Um verspätete Meldungen nach Art. 33 Abs. 1 DS-GVO zu vermeiden, empfehle ich allen verantwortlichen Stellen, intern schriftlich ein Verfahren zu fixieren, wie bei entsprechenden Vorfällen zu verfahren ist. Die Verfahrensanleitung soll dabei insbesondere Auskunft darüber geben:

– welche Personen und Fachbereiche wann und wie in entsprechenden Fällen einzubinden sind (z. B. auch die IT-Abteilung),
– wie die Vertretungsregelungen bei der Abwesenheit einzelner Personen sind,
– wie die Meldeprozesse im Detail durchgeführt werden sollen.

Hierbei ist wichtig, dass ein entsprechendes Dokument kein „totes“ Papier ist, sondern ständig aufgrund der gemachten Erfahrungen evaluiert und überarbeitet/ angepasst werden muss. Der Mitarbeiter, der an einem Freitag von einem entsprechenden Fall erfährt, soll auf diese Weise bestmöglich informiert und vorbereitet sein, auch wenn die Mehrzahl der Kollegen nicht mehr anwesend ist.

16. Arbeitsstatistik

Die statistische Aufgliederung der Arbeitsmenge in „Zahlen und Fakten“ (Ziff. 16.1) folgt den Vorgaben der Datenschutzkonferenz. Die Darstellung ist bundesweit einheitlich und wird u. a. der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht (Art. 59 DS-GVO). Sie ist allerdings nur bedingt aussagekräftig, da eine detaillierte Sicht der Dinge nicht erfolgt. Deshalb wird ergänzend die gewohnte detaillierte Struktur der Arbeitsstatistik fortgeführt (Ziff. 16.2 und 16.3).

16.1 Zahlen und Fakten

Zahlen und Fakten	**Fallzahlen 01.01.2019 bis 31.12.2019**
a. „Beschwerden“ Anzahl von Beschwerden, die im Berichtszeitraum nach DS-GVO eingegangen sind. Als Beschwerden werden bei Eingang solche Vorgänge gezählt, die schriftlich eingehen und bei der eine natürliche Person eine persönliche Betroffenheit darlegt, auf die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden“ werden nur dann gezählt, wenn sie verschriftlicht werden (z. B. durch Vermerk).	**5.081**
b. „Beratungen“ Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	**1.610**
c. „Meldungen von Datenschutzverletzungen“ Anzahl schriftlicher Meldungen.	**1.453**
d. „Abhilfemaßnahmen“* Anzahl der getroffenen Maßnahmen, die (1) nach Art. 58 Abs. 2a (Warnungen) (2) nach Art. 58 Abs. 2b (Verwarnungen) (3) nach Art. 58 Abs. 2c bis g und j (Anweisungen und Anordnungen) (4) nach Art. 58 Abs. 2i (Geldbußen) (5) nach Art. 58 Abs. 2h (Widerruf von Zertifizierungen) im Berichtszeitraum getroffen wurden.	(1) **1** (2) **13** (3) **8** (4) **6** (5) **0**
e. „Europäische Verfahren“ (1) Anzahl der Verfahren mit Betroffenheit (Art. 56) (2) Anzahl der Verfahren mit Federführung (Art. 56) (3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	(1) **243** (2) **12** (3) **66**

f. „Förmliche Begleitung bei Rechtsetzungsvorhaben“ Hier werden pauschaliert als Gesamtzahl die von Parlament/Regierung angeforderten und durchgeführten Beratungen genannt. Dies umfasst auch die Teilnahme in öffentlichen Ausschüssen und Stellungnahmen gegenüber Gerichten.	**12**

*Im Berichtsjahr wurden zudem **67** Ordnungswidrigkeitenverfahren wegen Verstößen gegen das BDSG a. F. und die DS-GVO abgeschlossen.

16.2
Ergänzende Erläuterungen zur Statistik „Zahlen und Fakten“

Für meine Arbeit wirklich aussagekräftig werden obigen Zahlen erst bei genauerer Spezifizierung und im Vergleich zum Vorjahr. Dem dienen die nachfolgende Tabelle und die Erläuterungen. Dabei werden die Zahlen bis bzw. ab 25.05.2018, dem Tag der Geltung der DS-GVO, zugrunde gelegt. Der berechnete monatliche Durchschnittswert soll dem besseren Verständnis und der Vergleichbarkeit angesichts der Übergangszeit im Vorjahr 2018 dienen.

Die Hoffnung, dass sich die Welle der Beschwerden und Beratungsgesuche nach eineinhalb Jahren DS-GVO beruhigen werde, erfüllte sich nur leicht. Hatte sich die Gesamtzahl der zu bearbeitenden Eingänge in 2018 nach dem Stichtag nahezu verdoppelt, war 2019 für das gesamte Jahr nur ein geringfügiger Rückgang zu verzeichnen. Die Aufgeregtheit des letzten Jahres ist einer sachlicheren Auseinandersetzung mit der neuen Rechtslage gewichen. Neue Schwerpunktthemen haben sich gebildet.

Spitzenreiter war in diesem Berichtsjahr die Zahl der Eingaben, die eine Datenschutzbeschwerde gegen Kreditinstitute zum Gegenstand haben. Wegen mehrerer Datenpannen erreichten mich in der Jahresmitte innerhalb weniger Tage ca. 650 Beschwerden gegen Mastercard (s. a. Ziff. I 11.2).

Beständig hoch ist die Zahl der Eingaben zu Auskunfteien und Inkassoinstituten, allen voran zur SCHUFA Holding AG (SCHUFA). Diese stand deshalb im Berichtsjahr besonders im datenschutzrechtlichen Fokus (s. a. Ziff. I 12.1).

Eine tendenzielle Steigerung zu den Vorjahren ist bei den Eingaben zum Themenkomplex Elektronische Kommunikation, Telemedien, Internet (social media) festzustellen. Es werden zunehmend kritische Fragen zum Umgang mit Betroffenenrechten bei Internetanbietern gestellt. Dies gilt auch im Bereich der Schulen, die sich vermehrt mit der Bitte um Beratung auch im IT-Bereich (s. a. Ziff. I 7.2) an mich wenden.

Der ungebrochene Trend zur privaten Videoüberwachung von Heim und Gut führt weiterhin zu entsprechenden Beschwerden von Nachbarn, Besuchern und Passanten.

Erfreulich ist, dass sich die internen behördlichen und betrieblichen Datenschutzbeauftragten offensichtlich mit den neuen Rechtsgrundlagen vertraut gemacht haben. Hier sind die Beratungsanfragen zurückgegangen.

Die telefonischen Beratungen spiegeln die Nachfragen wieder, die länger als zehn Minuten dauerten, keinen schriftlichen Niederschlag fanden, aber im Gespräch erledigt werden konnten. Hier wurde, wie in den Jahren davor, der Wert des Monats November, als Monat ohne besondere Vorkommnisse, als Durchschnittswert hochgerechnet. Dagegen ist der Aufwand für die schriftliche Erledigung von 823 Abgaben wegen fehlender Zuständigkeit im Berichtsjahr nicht gesondert ausgewiesen.

Die nachfolgende Übersicht stellt die Mengen der Eingaben, Beschwerden und Beratungen im Berichtsjahr im Vergleich zum Vorjahr dar:

Fachgebiete	Anzahl 2018		Anzahl 2019		
	01.01.2018 – 24.05.2018 ~ 5 Monate	25.05.2018 – 31.12.2018 ~ 7 Monate	01.01.2019 – 31.12.2019 = 12 Monate		
	Eingaben und Beschwerden und Beratungen) / mtl. Durchschnittswert zum Vergleich		Eingaben und Beschwerden	Beratung	Eingaben und Beschwerden und Beratungen / mtl. Durchschnittswert zum Vergleich
Kreditwirtschaft	54/10,8	178/25,4	949	10	959/79,9
Auskunfteien, Inkasso	118/23,6	533/76,2	923	19	942/78,5
e-Kommunikation, Internet	120/24	414/59,1	512	52	564/47
Schulen, Hochschulen, Archive	78/15,6	296/42,3	56	312	368/30,6
Videobeobachtung	Menge in den Fachthemen erfasst **	Menge in den Fachthemen erfasst**	253	95	348/29
Beschäftigtendatenschutz	59/11,8	197/28,1	199	131	330/27,5
Verkehr	39/7,8	134/19,1	240	39	279/23,3
Handel, Handwerk, Gewerbe	30/6	275/39,3	182	58	240/20
Betriebliche/Behördliche DSB	4/0,8	468/66,9	16	219	235/19,6
Kommunen, Wahlen	52/10,4	172/24,6	115	112	227/18,9
Adresshandel, Werbung	71/14,2	161/23	174	6	180/15
Polizei, Strafverfahren, Justiz, Verfassungsschutz	104/20,8	153/21,9	129	32	161/13,4
Gesundheit, Pflege	142/28,4	397/56,7	101	180	281/23,4
Vereine ,Verbände	16/3,2	323/46,1	57	77	134/11,1
Wohnen, Miete	148/29,6	248/35,4	54	66	120/10
Soziales	40/8	62/8,9	50	63	113/9,4
Versorgungsunternehmen	48/9,6	76/10,9	76	22	98/8,1
IT-Sicherheit, DV-Technik	30/6	54/7,7	30	57	87/7,3
Versicherungen	17/3,4	35/5	46	17	63/5,2
Rundfunk, Fernsehen, Presse	4/0,8	21/3	46	1	47/3,9
Datenschutz außerhalb DE/EU	0	5/0,7	3	6	9/0,75
Forschung, Statistik	10/2	4/0,6	10	1	11/0,9
Ausländerrecht	0	2/0,3	3	8	11/0,9
Steuerwesen*	4/0,8	7/1*	1	0	1/0,08*
Sonstige Themen < 10 (z. B. Religionen, Geodaten, Kammern)	33/6,6	141/20,1	33	27	60/5

BCR-Verfahren				17	17/1,4
Meldungen von Datenpannen	32/6,4	630/90			1.453/121,1
Gesamtsumme dokumentierter Eingaben und Beratungen und Datenpannen	**1.253/250,6**	**4.986/712**			**7.338/611,5**
zzgl. Summe telefonischer Beratungen	**2.420/484**	**4.739/677**			**7.044/587**
Gesamtsumme Eingaben und Beratungen	**3.673/734,6**	**9.725/1.389,3**			**14.382/1.198,5**

*Wesentliche Aufgabenbereiche der Steuerverwaltung gingen nach § 32h Abgabenordnung auf den BfDI über.

** Fälle der Videoüberwachung werden seit 2019 eigenständig erfasst.

Die Zahl der **Meldungen** von Datenschutzverletzungen **nach Art. 33 DS-GVO** sind von durchschnittlich 90 pro Monat auf 120 pro Monat gestiegen. Von den insgesamt 1.453 Meldungen waren die Bereiche Kreditwirtschaft, Auskunfteien, Handel und Gewerbe sowie der Gesundheitsbereich am stärksten betroffen. Die häufigsten gemeldeten Sachverhalte waren:

Fehlversand per Post, Fax und E-Mail	557 Fälle	(38,33 %)
Hackerangriff, Phishing, Schadsoftware	157 Fälle	(10,81 %)
Verlust/Diebstahl von Geräten, Datenträgern, Unterlagen	148 Fälle	(10,19 %)

Insbesondere ergaben sich aus einigen dieser Meldungen umfangreiche und zeitintensive Großberatungen über mehrere Termine. Es wurden Problemstellungen angetroffen, die die betroffenen Verantwortlichen mit ihren internen Datenschutzbeauftragten allein nicht zu lösen vermochten. Dies betraf z. B. Stadtwerke, Energieversorger, Bibliotheken, größere Schulen und eine Parkhausgesellschaft.

Auch die Nachfrage von global agierenden Unternehmen zur Genehmigung von sog. **Binding Corporate Rules (BCR)** ist deutlich gestiegen (s. a. Ziff. I 3.2). Mit den BCR geben sich die Unternehmen eigene rechtsverbindliche und durchsetzbare interne Vorschriften zum Schutz personenbezogener Daten, um Datenübermittlungen innerhalb der Unternehmensgruppe an Drittländer, die an und für sich kein angemessenes Datenschutzniveau bieten, zu ermöglichen. Diese Regeln müssen in einem europaweiten Kooperationsverfahren, also von Datenschutzaufsichtsbehörden mehrerer Mitgliedstaaten, gemeinsam geprüft werden und können nach erfolgter positiver Stellungnahme des Europäischen Datenschutzausschusses von der sog. federführenden Aufsichtsbehörde mit bindender Wirkung für die anderen Behörden genehmigt werden.

Bei allen in der Tabelle aufgeführten 17 BCR-Verfahren war meine Dienststelle für Deutschland die federführende Aufsichtsbehörde und in acht dieser Verfahren auch als sog. BCR Lead europaweit federführend.

Im Berichtsjahr bestand zudem noch erhöhter Beratungs- und Schulungsbedarf zu Themen der Datenschutz-Grundverordnung, deren neueren Entwicklungen und den zugehörigen IT-Fragen. In zahlreichen **Seminaren und Vorträgen** wurde von meinen Mitarbeiterinnen und Mitarbeitern bereichsspezifische Fachthemen (z. B. zu Bußgeldverfahren, zu Betroffenenrechte, zu Datenschutzverletzungen und Vorsorgemaßnahmen, zum internationalen Datenverkehr) an Anwender und Interessierte vermittelt. So hatte z. B. eine Mitarbeiterin von mir auch Gelegenheit, im Europarat auf der Konferenz der Kinderrechtskonvention zur Anwendung von Microsoft 365 in hessischen Schulen vorzutragen.

Weiterhin wurden drei **Referendarinnen und Referendare** in ihren Verwaltungsstationen ausgebildet.

16.3
Sanktionen

Offen waren zum Ende des Berichtszeitraums 80 eingeleitete Bußgeldverfahren. Im Berichtszeitraum wurden insgesamt 67 Ordnungswidrigkeitenverfahren, denen 32 Verstöße gegen das BDSG a. F. und 35 Verstöße nach DS-GVO zugrunde liegen, abgeschlossen. Damit konnten trotz der mit dem Wirksamwerden der DS-GVO andauernden erheblichen Arbeitsbelastung die meisten Rückstände aus den Vorjahren sowie einige Verfahren über Verstöße nach DS-GVO abschließend bearbeitet werden.

Insgesamt wurden sechs Verfahren mit einem Bußgeldbescheid beendet und Geldbußen in Höhe von insgesamt 19.500,00 EUR festgesetzt.

Den abgeschlossen Verfahren lagen eine Aufsichtspflichtverletzung nach § 130 OWiG wegen Verstoßes gegen § 34 BDSG a. F., eine entgegen § 4 f BDSG a. F. nicht erfolgte Bestellung eines Datenschutzbeauftragten, verspätete Meldungen nach Art. 33 DS-GVO und Verstöße gegen Art. 5 und 6 DS-GVO zugrunde.

16.4
Entwicklung der Anzahl von Meldungen nach Art. 33 DS-GVO seit dem 25.05.2018

In meinem 47. Tätigkeitsbericht habe ich unter Gliederungspunkt 4.11.3 das Thema „Meldungen der Verletzung des Schutzes personenbezogener

Daten“ (nachfolgend Datenpannen) ausführlich dargestellt. In diesem 48. Tätigkeitsbericht richte ich den Fokus auf die Entwicklung der Anzahl von gemeldeten Datenpannen seit dem 25.05.2018 sowie auf die möglichen Gründe für diese Entwicklung.

Im Jahr 2018 sind mir 630 Fälle von „Datenpannen“ nach Art. 33 DS-GVO gemeldet worden. Da diese über einen Zeitraum von etwas mehr als sieben Monaten erfolgten, handelte es sich um knapp 90 Meldungen pro Monat. Im 47. Tätigkeitsbericht hatte ich daher für das Jahr 2019 ca. 1.000 Meldungen prognostiziert.

Tatsächlich wurde diese Zahl im Jahr 2019 deutlich übertroffen. So sind im Jahr 2019 insgesamt 1.425 Meldungen nach Art. 33 DS-GVO bei meiner Behörde eingegangen. Damit bewegen sich die Meldungen auf einem deutlich höheren Niveau als im Jahr 2018. Im Berichtsjahr konnte ich monatlich knapp 120 gemeldete „Datenpannen“ verzeichnen und damit gegenüber 2018 etwa 30 Ereignisse monatlich mehr als 2018 (im Vergleich: 90 pro Monat im Jahr 2018).

Die hohe Anzahl von Meldungen führt in meiner Behörde natürlich zu einem deutlich höheren Arbeitsvolumen, da jede Meldung individuell geprüft werden muss. Selbst ähnlich gelagerte Fälle können nicht pauschal bewertet werden. Vielmehr muss den Umständen des jeweiligen Einzelfalls Rechnung getragen und die getroffenen Maßnahmen müssen umfassend überprüft werden.

Die Gründe für diesen signifikanten Anstieg der gemeldeten Fälle (>33,33 %) sind vielschichtig. So haben die Verantwortlichen seit dem 25.05.2018 mehr Erfahrung mit der Auslegung der DS-GVO sammeln können und neigen mittlerweile eher dazu, unregelmäßige Vorkommnisse auch als „Datenpannen“ zu identifizieren und entsprechend an die Aufsichtsbehörde zu melden.

Zum anderen ist der Anstieg sicher dem Inhalt der Norm selbst geschuldet. So sind die Voraussetzungen, die eine Pflicht zur Meldung an die Aufsichtsbehörde auslösen, deutlich niederschwelliger als unter dem BDSG-alt (vgl. TB 47, Gliederungspunkt 4.11.3).

Zudem werden derzeit, wenn auch in geringer Zahl (unter 2 %), Fälle gemeldet, bei denen die Voraussetzungen des Art. 33 DS-GVO nicht erfüllt sind. Bei derartigen Fällen erhalten die Verantwortlichen eine entsprechende Rückmeldung durch meine Behörde, in der erläutert wird, aus welchen Gründen der gemeldete Sachverhalt nicht meldepflichtig ist.

Zusätzlich spielt sicherlich auch die Regelung des Art. 83 Abs. 4 lit. a) DS-GVO in Bezug auf das Meldeverhalten eine Rolle, da das Unterlassen der Mitteilung eines meldepflichtigen Sachverhalts an die Aufsichtsbehörde

bußgeldbewehrt ist. Das Gleiche gilt für verspätete Meldungen sowie eine gegebenenfalls missachtete Dokumentationspflicht der Verantwortlichen, sofern nach erfolgter Prüfung und Risikoabwägung von einer Meldung abgesehen wird.

Nach alledem bleibt festzuhalten, dass das im Vorjahr bereits hohe Niveau der Zahl der gemeldeten Datenpannen nochmals angestiegen ist und zwar über das prognostizierte Maß hinaus.

17. Bilanzberichte

17.1
Das Projekt Hessenbox ist grundsätzlich abgeschlossen

Das von den hessischen Universitäten und dem hessischen Ministerium für Wissenschaft und Kunst seit dem Jahr 2016 verfolgte „Projekt Hessenbox", einer Cloud-Speicherlösung, die es universitätsübergreifend Nutzenden ermöglicht, auf sichere Weise Dokumente bereitzustellen, untereinander auszutauschen oder gemeinsam zu bearbeiten, ist im Rahmen der datenschutzrechtlichen Beurteilung abgeschlossen. Mit meiner Beteiligung und nach einer Reihe von Sitzungen in einem Zeitraum von mehr als drei Jahren mit den Trägern des Verfahrens und entsprechender Verarbeitungstätigkeit konnte eine einvernehmliche und den Belangen des Datenschutzes Rechnung tragende Lösung für das Dokumentenmanagement- und Kommunikationssystem gefunden werden. Für die Universitätsverwaltungen und Lehrenden sowie für die Studierenden ist damit ein Instrument geschaffen worden, das in dieser Form hessenweit einmalig ist.

Über das Projekt habe ich im 46. Tätigkeitsbericht (Ziff. 16.1) ausführlich berichtet. Seit dieser Zeit haben weitere Zusammenkünfte stattgefunden, die nun zu einem datenschutzrechtlichen Abschluss geführt haben. Dabei wurde von mir berücksichtigt, dass eine zusätzliche Funktionalität mit Namen „OnlyOffice" kurzfristig noch in die Anwendung Hessenbox implementiert wurde. Hersteller dieser Software ist Ascensio System SIA mit Hauptsitz in Riga, Lettland. Bei OnlyOffice handelt es sich um eine optionale Funktion, die in die Software-Lösung PowerFolder (siehe hierzu ebenfalls 16. TB, Ziff. 16.1) integriert und aktiviert werden kann. Geschäftsbedingungen zum Einsatz der OnlyOffice Integration Edition sind unter https://help.onlyoffice.com/products/files/doceditor.aspx?fileid=4995927&doc=bTNVWUNPTm1yM-zBlRW9Eb3o1MityMWJRNGlzcTFCZFlxdFRLbEFLdmVOcz0_IjQ5OTU5Mjci0 einzusehen (letzter Aufruf: 14.01.2020). Eine datenschutzrechtliche Erklärung in englischer Sprache des Herstellers von OnlyOffice findet sich im Web unter https://www.onlyoffice.com/blog/2018/05/how-onlyoffice-complies-with-gdpr/ (letzter Aufruf: 14.01.2020), in der auch einige Fragen zur Datensicherheit beantwortet sind.

Eine entsprechende deutschsprachige Adaption ist in den Nutzungsbedingungen der jeweiligen Hochschule zu erwarten.

Mit Hilfe von OnlyOffice können die Nutzenden der Hessenbox auch Office-Dokumente direkt im Browser anzeigen und darüber hinaus auch kollaborativ mit anderen (für den Zugriff auf das Dokument in der Hessenbox

berechtigten) Nutzenden an einem Dokument arbeiten. Für die Nutzung sind separate Lizenzen und ein eigener Server notwendig.

Der OnlyOffice-Server wird zentral an der Universität Gießen betrieben und von allen Betreiber-Standorten genutzt. Bei Nutzung der Funktion wird das Dokument an den OnlyOffice-Server zur Darstellung bzw. zum kollaborativen Arbeiten übertragen und nach Beendigung erneut am Betreiber-Standort (versioniert) gesichert. Die Übertragung der Dateien zwischen den Standorten findet ausschließlich SSL-verschlüsselt (TLS 1.2 oder höher) über das Hessennetz (VPN) statt. Die Übertragung zur Darstellung und während der Bearbeitung im Browser ist ebenfalls SSL-verschlüsselt (TLS 1.2 oder höher).

Die Projektleitung Hessenbox konnte mich von dem Mehrwert der Anwendung für die Nutzenden der Hessenbox überzeugen. Da in diesem Zusammenhang keine negativen Auswirkungen für Datenschutz und Datensicherheit zu befürchten sind, habe ich der Erweiterung der Anwendung Hessenbox um die Funktionalität OnlyOffice zugestimmt.

Über die Jahre hinweg haben sich sowohl die Vertreter der an dem Projekt beteiligten Universitäten als auch die des hessischen Ministeriums für Wissenschaft und Kunst kompetent und zielgerichtet den hohen Anforderungen der datenschutzrechtlichen Komponenten gestellt. Erschwerend kam hinzu, dass im Verlauf des Projekts die Datenschutz-Grundverordnung ihre Wirksamkeit erzielte. Das bedeutete u. a., die bisher erstellten Verfahrensverzeichnisse nach § 6 Hessisches Datenschutzgesetz (alt) auf Verarbeitungsverzeichnisse nach Art. 30 DS-GVO umzuschreiben oder aber die Informationen i. S. v. Art. 13 und 14 DS-GVO nachzubessern bzw. zu erweitern. In diesem Zusammenhang hat die Arbeitsgruppe Dokumente erstellt, welche die Ablaufprozesse darstellen, um den erhöhten Anforderungen der DS-GVO gerecht zu werden. Diese Dokumente können für weitere, insbesondere Kooperationsprojekte im Bereich der Hochschulen als Vorlage dienen sowie in größerem Umfang weiterverwendet werden. Die konstruktive Zusammenarbeit der Entscheidungsträger hat entscheidend dazu beigetragen, das universitätsübergreifende Verfahren Hessenbox zu einem erfolgreichen Abschluss zu führen.

17.2
Das länderübergreifende Projekt „Digitales Lernen unterwegs“ nimmt weitere Hürden

Das Projekt „Digitales Lernen unterwegs“ (DigLu), das die Betreuung der schulischen Laufbahn von Kindern beruflich Reisender verbessern soll, kann als Pilotverfahren starten.

In den vergangenen Tätigkeitsberichten habe ich regelmäßig über die Fortschritte bei der Entwicklung des länderübergreifenden Projekts DigLu (Digitales Lernen unterwegs) berichtet (siehe 47. Tätigkeitsbericht, Ziff. 5.1 und 46. Tätigkeitsbericht, Ziff. 9.2). Die datenschutzrechtlichen Anforderungen an das Pilotprojekt waren enorm (siehe 46. Tätigkeitsbericht, Ziff. 9.2.3), konnten jedoch von der Projektgruppe DigLu, einer länderübergreifenden Arbeitsgruppe unter Führung von Nordrhein-Westfalen, Schritt für Schritt umgesetzt werden.

Die aktuellen Bemühungen gelten einem Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO, den die an dem Pilotprojekt beteiligten Länder bzw. Bildungsministerien mit dem Dienstleister Jordy Media abschließen sollen. Dabei kommt es zu der Besonderheit, dass sowohl die Länder als auch die Schulen Vertragspartner des Dienstleisters, der die Software und in einem Unterauftragsverhältnis die Hardware (also die Rechenzentrumsleistung) zur Verfügung stellt, sind. Vorgesehen ist, den Schulen online im Rahmen der Anmeldung zum Verfahren den Vertragsabschluss zu ermöglichen, während die Ministerien dies in klassischer Schriftform umsetzen.

Die Projektgruppe DigLu plant, im Sommerschuljahr 2020 das Verfahren in einzelnen Verfahrensschritten auszurollen. Die technischen, administrativen und datenschutzrechtlichen Parameter für den Betrieb des Verfahrens sind formuliert und in einer Verfahrensdokumentation verschriftlicht. Die Frage, ob eine Datenschutz-Folgenabschätzung (DSFA) gem. Art. 35 DS-GVO erforderlich ist, entscheidet sich maßgeblich an Art und Inhalt der personenbezogenen Daten der Schüler, die mit DigLu verarbeitet werden. In der ersten Umsetzungsphase des Piloten sind die Dateninhalte auf ein Minimum reduziert, so dass eine DSFA obsolet erscheint. Sollte zu einem späteren Zeitpunkt z. B. der Datenkranz erweitert werden oder das Verfahren sich inhaltlich ändern, wäre eine erneute Prüfung hinsichtlich des Erfordernisses zur Durchführung einer DSFA erforderlich.

Das als Pilot auf zwei Jahre ausgelegte Projekt soll nach dem ersten zeitlichen Abschnitt evaluiert werden, um mögliche Schlussfolgerungen für den weiteren Betrieb des Verfahrens zu ziehen sowie dessen Erweiterung auf andere Länder erfolgen zu lassen. Schließlich sollen in den kommenden Jahren die bislang noch nicht beteiligten Länder dem Verfahren beitreten können.

Anhang I

Materialien zum Datenschutz

1. Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

1.1
Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019[1] – Unternehmen haften für Datenschutzverstöße ihrer Beschäftigten!

Unternehmen haften im Rahmen von Art. 83 Datenschutz-Grundverordnung (DS-GVO) für schuldhafte Datenschutzverstöße ihrer Beschäftigten, sofern es sich nicht um einen Exzess handelt. Dabei ist nicht erforderlich, dass für die Handlung ein gesetzlicher Vertreter oder eine Leitungsperson verantwortlich ist. Zurechnungseinschränkende Regelungen im nationalen Recht würden dem widersprechen.

Diese Haftung für Mitarbeiterverschulden ergibt sich aus der Anwendung des sogenannten funktionalen Unternehmensbegriffs des europäischen Primärrechts. Der funktionale Unternehmensbegriff aus dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV) besagt, dass ein Unternehmen jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung ist. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend darauf hin. Nach der Rechtsprechung zum funktionalen Unternehmensbegriff haften Unternehmen für das Fehlverhalten sämtlicher ihrer Beschäftigten. Eine Kenntnis der Geschäftsführung eines Unternehmens von dem konkreten Verstoß oder eine Verletzung der Aufsichtspflicht ist für die Zuordnung der Verantwortlichkeit nicht erforderlich. Handlungen von Beschäftigten, die bei verständiger Würdigung nicht dem Kreis der jeweiligen unternehmerischen Tätigkeit zugerechnet werden können („Exzesse“), sind ausgenommen.

Die alten nationalen Haftungsregeln wurden bisher nicht europarechtskonform der neuen Rechtslage angepasst. Unzutreffend verweist § 41 Abs. 1 des neuen Bundesdatenschutzgesetzes (BDSG) auf zurechnungseinschränkende Regelungen im OWiG. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben bereits im Rahmen des Gesetzgebungsverfahrens zum neuen Bundesdatenschutzgesetz darauf aufmerksam gemacht, dass diese Bestimmungen den Vorgaben der DS-GVO zur Verantwortlichkeit für Datenschutzverstöße widersprechen.

1 Gegen die Stimmen von Bayern und Baden-Württemberg.

Die DSK begrüßt insoweit, dass der Koalitionsvertrag vorsieht, das Sanktionsrecht für Unternehmen generell im deutschen Recht so zu ändern, dass „die von Fehlverhalten von Mitarbeiterinnen und Mitarbeitern profitierenden Unternehmen stärker sanktioniert werden“. Diese gebotene Modernisierung des deutschen Unternehmenssanktionsrechts entspräche dann auch dem europäischen Kartellrecht und dem etablierten internationalen Standard.

Die DSK fordert den Bundesgesetzgeber daher nochmals auf, in den Beratungen des Entwurfs des Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 die §§ 30, 130 OWiG klarstellend vom Anwendungsbereich auszunehmen und damit dem europäischen Recht anzupassen.

1.2
Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Hambacher Schloss – 3. April 2019

Hambacher Erklärung zur Künstlichen Intelligenz Sieben datenschutzrechtliche Anforderungen

Systeme der Künstlichen Intelligenz (KI) stellen eine substanzielle Herausforderung für Freiheit und Demokratie in unserer Rechtsordnung dar. Entwicklungen und Anwendungen von KI müssen in demokratisch-rechtsstaatlicher Weise den Grundrechten entsprechen. Nicht alles, was technisch möglich und ökonomisch erwünscht ist, darf in der Realität umgesetzt werden. Das gilt in besonderem Maße für den Einsatz von selbstlernenden Systemen, die massenhaft Daten verarbeiten und durch automatisierte Einzelentscheidungen in Rechte und Freiheiten Betroffener eingreifen. Die Wahrung der Grundrechte ist Aufgabe aller staatlichen Instanzen. Wesentliche Rahmenbedingungen für den Einsatz von KI sind vom Gesetzgeber vorzugeben und durch die Aufsichtsbehörden zu vollziehen. Nur wenn der Grundrechtsschutz und der Datenschutz mit dem Prozess der Digitalisierung Schritt halten, ist eine Zukunft möglich, in der am Ende Menschen und nicht Maschinen über Menschen entscheiden.

I.
Künstliche Intelligenz und Datenschutz

„Künstliche Intelligenz“ (auch „KI“ oder „Artificial Intelligence“ – „AI“) wird derzeit intensiv diskutiert, da sie neue Wertschöpfung in vielen Bereichen von Wirtschaft und Gesellschaft verspricht. Die Bundesregierung hat eine KI-Strategie veröffentlicht, mit dem Ziel, Deutschland an die Weltspitze

der Entwicklung von KI zu bringen. „AI made in Germany“ soll gleichzeitig dafür sorgen, dass auch bei weitreichendem Einsatz Künstlicher Intelligenz die Grundwerte und Freiheitsrechte, die in Deutschland und der EU gelten, weiterhin die prägende Rolle für unser Zusammenleben spielen. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßen diesen Ansatz der grundrechtsverträglichen Gestaltung von KI ausdrücklich.

Eine allgemein anerkannte Definition des Begriffs der Künstlichen Intelligenz existiert bisher nicht. Nach dem Verständnis der Bundesregierung geht es bei KI darum, „technische Systeme so zu konzipieren, dass sie Probleme eigenständig bearbeiten und sich dabei selbst auf veränderte Bedingungen einstellen können. Diese Systeme haben die Eigenschaft, aus neuen Daten zu ‚lernen‘ […].“[2]

KI-Systeme werden beispielsweise bereits in der Medizin unterstützend in Forschung und Therapie eingesetzt. Schon heute sind neuronale Netze in der Lage, automatisch komplexe Tumorstrukturen zu erkennen. KI-Systeme können auch genutzt werden, um Depressionserkrankungen anhand des Verhaltens in sozialen Netzwerken oder anhand der Stimmmodulation beim Bedienen von Sprachassistenten zu erkennen. In den Händen von Ärzten kann dieses Wissen dem Wohl der Erkrankten dienen. In den falschen Händen jedoch kann es auch missbraucht werden.

Auch zur Bewertung von Bewerbungsunterlagen wurde bereits ein KI-System eingesetzt, mit dem Ziel, frei von menschlichen Vorurteilen zu entscheiden. Allerdings hatte das Unternehmen bislang überwiegend männliche Bewerber eingestellt und das KI-System mit deren erfolgreichen Bewerbungen trainiert. In der Folge bewertete das KI-System Frauen sehr viel schlechter, obwohl das Geschlecht nicht nur kein vorgegebenes Bewertungskriterium, sondern dem System sogar unbekannt war. Dies offenbart die Gefahr, dass in Trainingsdaten abgebildete Diskriminierungen nicht beseitigt, sondern verfestigt werden.

Anhand dieser Beispiele wird deutlich, dass mit KI-Systemen häufig personenbezogene Daten verarbeitet werden und diese Verarbeitung Risiken für die Rechte und Freiheiten von Menschen birgt. Sie zeigen auch, wie wichtig es ist, Entwicklung und Einsatz von KI-Systemen politisch, gesellschaftlich und rechtlich zu begleiten. Die unabhängigen Datenschutzaufsichtsbehörden

2 BT-Drs. 19/1982 zu 1.: Die Datenethikkommission der Bundesregierung hebt ergänzend als wichtige Grundlagen für KI die Mustererkennung, das maschinelle Lernen und Methoden der heuristischen Suche, der Inferenz und der Handlungsplanung hervor (Empfehlungen der Datenethikkommission für die Strategie Künstliche Intelligenz der Bundesregierung, 9.10.2018).

des Bundes und der Länder verstehen die folgenden Anforderungen als einen konstruktiven Beitrag zu diesem zentralen gesellschaftspolitischen Projekt.

II.
Datenschutzrechtliche Anforderungen an Künstliche Intelligenz

Für die Entwicklung und den Einsatz von KI-Systemen, in denen personenbezogene Daten verarbeitet werden, beinhaltet die Datenschutz-Grundverordnung (DS-GVO) wichtige rechtliche Vorgaben. Sie dienen dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen. Auch für KI-Systeme gelten die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO). Diese Grundsätze müssen gemäß Art. 25 DS-GVO durch frühzeitig geplante technische und organisatorische Maßnahmen von den Verantwortlichen umgesetzt werden (Datenschutz durch Technikgestaltung).

1. KI darf Menschen nicht zum Objekt machen

Die Garantie der Würde des Menschen (Art. 1 Abs. 1 GG, Art. 1 GRCh) gebietet, dass insbesondere im Fall staatlichen Handelns mittels KI der Einzelne nicht zum Objekt gemacht wird. Vollständig automatisierte Entscheidungen oder Profiling durch KI-Systeme sind nur eingeschränkt zulässig. Entscheidungen mit rechtlicher Wirkung oder ähnlicher erheblicher Beeinträchtigung dürfen gemäß Art. 22 DS-GVO nicht allein der Maschine überlassen werden. Wenn der Anwendungsbereich des Art. 22 DS-GVO nicht eröffnet ist, greifen die allgemeinen Grundlagen des Art. 5 DS-GVO, die insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zurechenbarkeit und Fairness die Rechte des Einzelnen schützen. Betroffene haben auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (Intervenierbarkeit), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung.

2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

Auch für KI-Systeme gilt, dass sie nur zu verfassungsrechtlich legitimierten Zwecken eingesetzt werden dürfen. Zu beachten ist auch der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO). Zweckänderungen sind mit Art. 6 Abs. 4 DS-GVO klare Grenzen gesetzt. Auch bei KI-Systemen müssen erweiterte Verarbeitungszwecke mit dem ursprünglichen Erhebungszweck vereinbar sein. Das gilt auch für die Nutzung personenbezogener Daten zu Trainingszwecken von KI-Systemen.

3. KI muss transparent, nachvollziehbar und erklärbar sein

Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO). Dies erfordert insbesondere eine transparente Verarbeitung, bei der die Informationen über den Prozess der Verarbeitung und ggf. auch über die verwendeten Trainingsdaten leicht zugänglich und verständlich sind (Art. 12 DS-GVO). Entscheidungen, die auf Grundlage des Einsatzes von KI-Systemen erfolgen, müssen nachvollziehbar und erklärbar sein. Es genügt nicht die Erklärbarkeit im Hinblick auf das Ergebnis, darüber hinaus muss die Nachvollziehbarkeit im Hinblick auf die Prozesse und das Zustandekommen von Entscheidungen gewährleistet sein. Nach der DS-GVO ist dafür auch über die involvierte Logik ausreichend aufzuklären. Diese Transparenz-Anforderungen sind fortwährend zu erfüllen, wenn KI-Systeme zur Verarbeitung von personenbezogenen Daten eingesetzt werden. Es gilt die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO).

4. KI muss Diskriminierungen vermeiden

Lernende Systeme sind in hohem Maße abhängig von den eingegebenen Daten. Durch unzureichende Datengrundlagen und Konzeptionen kann es zu Ergebnissen kommen, die sich als Diskriminierungen auswirken. Diskriminierende Verarbeitungen stellen eine Verletzung der Rechte und Freiheiten der betroffenen Personen dar. Sie verstoßen u. a. gegen bestimmte Anforderungen der Datenschutz-Grundverordnung, etwa den Grundsatz der Verarbeitung nach Treu und Glauben, die Bindung der Verarbeitung an legitime Zwecke oder die Angemessenheit der Verarbeitung.

Diese Diskriminierungsneigungen sind nicht immer von vornherein erkennbar. Vor dem Einsatz von KI-Systemen müssen deshalb die Risiken für die Rechte und Freiheiten von

Personen mit dem Ziel bewertet werden, auch verdeckte Diskriminierungen durch Gegenmaßnahmen zuverlässig auszuschließen. Auch während der Anwendung von KI-Systemen muss eine entsprechende Risikoüberwachung erfolgen.

5. Für KI gilt der Grundsatz der Datenminimierung

Für KI-Systeme werden typischerweise große Bestände von Trainingsdaten genutzt. Für personenbezogene Daten gilt dabei auch in KI-Systemen der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO). Die Verarbeitung personenbezogener Daten muss daher stets auf das notwendige Maß beschränkt sein. Die Prüfung der Erforderlichkeit kann ergeben, dass

die Verarbeitung vollständig anonymer Daten zur Erreichung des legitimen Zwecks ausreicht.

6. KI braucht Verantwortlichkeit

Die Beteiligten beim Einsatz eines KI-Systems müssen die Verantwortlichkeit ermitteln und klar kommunizieren und jeweils die notwendigen Maßnahmen treffen, um die rechtmäßige Verarbeitung, die Betroffenenrechte, die Sicherheit der Verarbeitung und die Beherrschbarkeit des KI-Systems zu gewährleisten. Der Verantwortliche muss sicherstellen, dass die Grundsätze nach Art. 5 DS-GVO eingehalten werden. Er muss seine Pflichten im Hinblick auf die Betroffenenrechte aus Art. 12 ff DS-GVO erfüllen. Der Verantwortliche muss die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO gewährleisten und somit auch Manipulationen durch Dritte, die sich auf die Ergebnisse der Systeme auswirken, verhindern. Beim Einsatz eines KI-Systems, in dem personenbezogene Daten verarbeitet werden, wird in der Regel eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich sein.

7. KI benötigt technische und organisatorische Standards

Um eine datenschutzgerechte Verarbeitung sicherzustellen, sind für Konzeption und Einsatz von KI-Systemen technische und organisatorische Maßnahmen gem. Art. 24 und 25 DS-GVO zu treffen, wie z. B. Pseudonymisierung. Diese erfolgt nicht allein dadurch, dass der Einzelne in einer großen Menge personenbezogener Daten scheinbar verschwindet. Für den datenschutzkonformen Einsatz von KI-Systemen gibt es gegenwärtig noch keine speziellen Standards oder detaillierte Anforderungen an technische und organisatorische Maßnahmen. Die Erkenntnisse in diesem Bereich zu mehren und Best-Practice-Beispiele zu entwickeln ist eine wichtige Aufgabe von Wirtschaft und Wissenschaft. Die Datenschutzaufsichtsbehörden werden diesen Prozess aktiv begleiten.

III.
Die Entwicklung von KI bedarf der Steuerung

Die Datenschutzaufsichtsbehörden überwachen die Anwendung des Datenschutzrechts, setzen es durch und haben die Aufgabe, bei der Weiterentwicklung für einen effektiven Grundrechtsschutz einzutreten. Angesichts der hohen Dynamik in der Entwicklung der Technologien von Künstlicher Intelligenz und der vielfältigen Einsatzfelder zeichnen sich die Grenzen der Entwicklung noch nicht ab. Gleichermaßen sind die Risiken der

Verarbeitung personenbezogener Daten in KI-Systemen nicht pauschal einzuschätzen. Auch ethische Grundsätze sind zu beachten. Wissenschaft, Datenschutzaufsichtsbehörden, die Anwender und besonders die Politik sind gefordert, die Entwicklung von KI zu begleiten und im Sinne des Datenschutzes zu steuern.

1.3
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 23. April 2019

Keine Abschaffung der Datenschutzbeauftragten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) spricht sich gegen eine Abschaffung oder Verwässerung der die Datenschutzgrundverordnung ergänzenden nationalen Regelungen der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten aus.

Nach § 38 Bundesdatenschutzgesetz müssen z. B. Unternehmen und Vereine Datenschutzbeauftragte benennen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Diese Pflicht hat sich seit vielen Jahren bewährt und ist deshalb auch bei der Datenschutzreform im deutschen Recht beibehalten worden.

Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße schon im Vorfeld zu vermeiden und das Sanktionsrisiko gering zu halten. Dies hat sich ganz besonders bei der Umstellung auf die Datenschutz-Grundverordnung bewährt.

Auch beim Wegfall der nationalen Benennungspflicht von Datenschutzbeauftragten bleiben die Pflichten des Datenschutzrechts bestehen. Verantwortliche verlieren jedoch interne Beraterinnen und Berater zu Fragen des Datenschutzes. Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren.

Eine Aufweichung dieser Benennungspflicht, insbesondere für kleinere Unternehmen und Vereine, wird diese daher nicht entlasten, sondern ihnen mittelfristig schaden.

1.4
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12. September 2019

Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten!

Die Bundesregierung will die in der Verwaltung geführten Register modernisieren und plant in diesem Zusammenhang einen einfacheren Zugriff auf dort gespeicherte personenbezogene Daten. Nach Auffassung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) darf dieses Vorhaben nicht zur Einführung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren führen. Vielmehr muss der Schutz der Grundrechte und Grundfreiheiten, insbesondere das Recht auf Schutz personenbezogener Daten, Priorität haben. Ebenso wichtig ist es, den Bürgerinnen und Bürgern die besseren Dienstleistungen verbunden mit einer deutlich höheren Transparenz anzubieten.

Bundesregierung nimmt Modernisierung der Register in Angriff

Die Bundesregierung hat mit dem Onlinezugangsgesetz ein umfangreiches Digitalisierungsprogramm für die Verwaltung in Deutschland gestartet. Bund und Länder sind verpflichtet, ihre Verwaltungsleistungen künftig auch elektronisch über Verwaltungsportale anzubieten. Es sollen Nutzerkonten bereitgestellt werden, über die sich Nutzende für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.

In diesem Zusammenhang hat sich der Nationale Normenkontrollrat (NKR) für eine Modernisierung der deutschen Registerlandschaft ausgesprochen und empfohlen, dass bestimmte Basisdaten von Bürgern und Unternehmen nur einmal mitgeteilt werden müssen („Once Only"-Prinzip). Der NKR hat darüber hinaus angeregt, datenschutzkonforme Identifikationsnummern für Personen, Unternehmen sowie Gebäude, Wohnungen und Flurstücke zu schaffen und zu nutzen und ein „Datencockpit" einzurichten, bei dem die Bürgerinnen und Bürger alle staatlichen Datenflüsse im Auge haben können.

Die Einführung solcher Identifikationsnummern für Personen wird aktuell unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI) von der Bundesregierung verfolgt. Der IT-Planungsrat hat in seiner 28. Sitzung am 12. März 2019 den vom BMI vorgelegten „Leitlinien für eine Modernisierung der Registerlandschaft" zugestimmt sowie den „Vorschlag

für die Verbesserung des Identitätsmanagements als Teil der Registermodernisierung“ zur Kenntnis genommen und das angestrebte Vorhaben begrüßt.

Datenschutzfreundliche und transparente Gestaltung für Bürgerinnen und Bürger

Bereits die Schaffung einheitlicher und verwaltungsübergreifender Personenkennzeichen bzw. Identifikatoren und einer entsprechenden Infrastruktur zum Datenaustausch bergen die Gefahr, dass personenbezogene Daten in großem Maße leicht zusammengetragen, verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden könnten. Die Datenschutzkonferenz weist darauf hin, dass das Bundesverfassungsgericht schon seit Jahrzehnten der Einführung und Verarbeitung derartiger Personenkennzeichen sehr enge Schranken auferlegt, da sie massiv in den Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffener Bürgerinnen und Bürger eingreifen. Bereits die Möglichkeit einer umfassenden Katalogisierung von Bürgerinnen und Bürgern durch den Staat gefährdet das Persönlichkeitsrecht, da sie bei den Menschen zu einer vorauseilenden Anpassung ihres Verhaltens führen kann. Auch die Grundsätze der europäischen Datenschutz-Grundverordnung und deren Regelungen zur datenschutzgerechten Gestaltung setzen einheitlichen und verwaltungsübergreifenden Personenkennzeichen enge Grenzen und verlangen geeignete Garantien für die Wahrung der Rechte und Freiheiten der betroffenen Personen.

Insbesondere im Hinblick auf die geplante Verwendung modernisierter Register für zukünftige Zensus-Erhebungen und geplante/modernisierte Zugriffsrechte der Sicherheitsbehörden bedarf es eines besonderen Schutzes der betroffenen Personen. Den hohen Risiken für das Recht auf informationelle Selbstbestimmung muss in einem umfassenden regulatorischen, vor allem aber technischen und organisatorischen Konzept begegnet werden. Nur so können die vom deutschen und europäischen Verfassungsrecht geforderten Garantien gewahrt werden.

Die Modernisierung der Register muss zwingend von Beginn an auch dafür genutzt werden, den Bürgerinnen und Bürgern die Nutzung der im Online-Zugangsgesetz vorgesehenen Dienstleistungen durch Nutzung einmal hinterlegter Daten zu erleichtern. Von besonderer Bedeutung ist es darüber hinaus, den Bürgerinnen und Bürgern ein im Vergleich zur gegenwärtigen Situation deutlich höheres Maß an Transparenz zu gewährleisten. Ein „Datencockpit“, wie es der NKR bereits vorgeschlagen hat, muss es den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welches Register welche Daten über sie vorhält, welche Behörden darauf zugegriffen haben und mit welchen anderen Daten diese verknüpft wurden. Gleichzeitig muss gewähr-

leistet sein, dass ausschließlich den betroffenen Bürgerinnen und Bürgern der Zugriff möglich ist. Auf dieser Grundlage muss die Digitalisierung der Verwaltung dazu genutzt werden, das informationelle Machtgefälle zwischen Staat und Bürgerinnen und Bürgern weitgehend aufzuheben und ihnen die Inanspruchnahme ihrer Rechte deutlich zu erleichtern.

Dazu muss nach Auffassung der Datenschutzkonferenz die dezentrale Registerstruktur erhalten bleiben. Die Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern lehnt die Datenschutzkonferenz ab. Sie fordert alternative Methoden zur eindeutigen Identifizierung. Neben Abgleichen über den jeweiligen Datensatz des Registers kämen dafür allenfalls sektorspezifische Personenkennziffern in Betracht, die eine eindeutige Identifizierung erlauben, einseitigen staatlichen Abgleich von Daten verhindern, ein Höchstmaß an Transparenz beispielsweise durch ein Datencockpit ermöglichen, das Risiko von Missbrauch und Kompromittierung verringern und die Eindeutigkeit von Registern gewährleisten.

1.5
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06. November 2019

Empfehlungen für eine datenschutzkonforme Gestaltung von KI-Systemen

Auf der Grundlage der Hambacher Erklärung vom 03.04.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in einem Positionspapier Anforderungen an KI-Systeme erarbeitet, deren Umsetzung die DSK für eine datenschutzkonforme Gestaltung von KI-Systemen empfiehlt. Die in der Hambacher Erklärung festgelegten rechtlichen Rahmenbedingungen werden damit im Hinblick auf technische und organisatorische Maßnahmen konkretisiert, die auf die unterschiedlichen Phasen der Lebenszyklen von KI-Systemen bezogen sind.

Die Phasen des Lebenszyklus eines KI-Systems – Designs des KI-Systems, Veredelung von Rohdaten zu Trainingsdaten, Training der KI-Komponenten, Validierung der Daten und KI-Komponenten sowie des KI-Systems, Einsatz des KI-Systems und die Rückkopplung von Ergebnissen – werden am Maßstab von Gewährleistungszielen untersucht. Um aus rechtlichen Anforderungen KI-spezifische technische und organisatorische Maßnahmen abzuleiten und zu systematisieren, werden die Gewährleistungsziele Transparenz, Datenmi-

nimierung, Nichtverkettung, Intervenierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit verwendet.

Für die Verarbeitung von personenbezogenen Daten, bei der KI-Systeme zum Einsatz kommen, gelten die in der DS-GVO formulierten Grundsätze. Mit dem Positionspapier wird Verantwortlichen im Umfeld von KI ein Handlungsrahmen für die datenschutzrechtlichen Vorgaben an die Hand gegeben, an dem sie sich bei der Planung und dem Betrieb von KI-Systemen orientieren können. Das Positionspapier soll verdeutlichen, dass der Einsatz von KI-Systemen und der Datenschutz keine zwingenden Gegensätze sind. Die Chancen und neuen Möglichkeiten des Einsatzes von KI-Systemen werden durch einen modernen Datenschutz nicht verhindert. Das Positionspapier soll die Entwicklung und den Einsatz von KI auch unter Nutzung personenbezogener Daten konstruktiv begleiten. Damit wird Handlungssicherheit gesteigert und sichergestellt, dass die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere das Recht auf informationelle Selbstbestimmung, auch in dem dynamischen, von KI-Systemen geprägten Umfeld gewahrt werden.

Die DSK legt dieses Positionspapier auch vor, um den Dialog mit den relevanten Akteuren aus Politik, Wirtschaft, Wissenschaft und Gesellschaft wie den Verbrauchervereinigungen auf dieser Grundlage weiter zu intensivieren.

Hinweis HBDI: Wegen des großen Umfangs des Positionspapiers wurde auf den Abdruck verzichtet. Es ist unter https://www.datenschutzkonferenz-online.de, dem offiziellen Webauftritt der Datenschutzkonferenz (DSK), zu finden.

1.6
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06. November 2019

Gesundheitseinrichtungen müssen unabhängig von ihrer Größe den Schutz von Patientendaten gewährleisten

Die Datenschutzkonferenz weist nachdrücklich darauf hin, dass die Sicherheit von Patientendaten in der medizinischen Behandlung nach der Datenschutz-Grundverordnung flächendeckend gewährleistet sein muss. Der effektive Schutz von Gesundheitsdaten darf nicht von der Größe der Versorgungseinrichtung abhängen.

In der jüngeren Vergangenheit häufen sich Vorfälle, in denen der Schutz von Patientendaten in der stationären Versorgung gefährdet ist. So wurden im Juli 2019 eine Reihe von Einrichtungen eines Trägers in Rheinland-Pfalz und dem Saarland Opfer eines Befalls mit Schadsoftware. Die durch diese erfolgte Verschlüsselung von Daten im IT-Verbund der Trägergesellschaft

hat zu weitreichenden Beeinträchtigungen des Krankenhausbetriebs geführt. Im September 2019 wurde bekannt, dass weltweit mehr als 16 Millionen Datensätze, darunter 13.000 von in deutschen Gesundheitseinrichtungen behandelten Patienten, offen im Internet zugänglich waren. Ursache hierfür waren nach den bislang bekannt gewordenen Informationen insbesondere unzureichende technische und organisatorische Vorkehrungen zum Schutz dieser Daten.

Der Einsatz von Informations- und Kommunikationstechnik in der Gesundheitsversorgung ist im Zeitalter der digitalisierten Medizin unabdingbar. Allerdings müssen die in diesem Zusammenhang rechtlich gebotenen und nach dem Stand der Technik angemessenen Vorkehrungen zu einem effektiven Schutz der Daten von Patientinnen und Patienten flächendeckend getroffen werden. Dazu sind alle in diesem Zusammenhang tätigen Einrichtungen unabhängig von ihrer Größe aufgrund der Datenschutz-Grundverordnung verpflichtet.

Die Datenschutzkonferenz fordert vor dem Hintergrund einer zunehmenden Digitalisierung der Gesundheitsversorgung und angesichts der damit einhergehenden Gefährdungen ausdrücklich dazu auf, auch in finanzieller Hinsicht sicherzustellen, dass alle Einrichtungen des Gesundheitswesens die zum Schutz der Patientendaten nach dem Stand der Technik gesetzlich gebotenen Vorkehrungen ergreifen können.

1.7
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06. November 2019

Gesundheitswebseiten und Gesundheits-Apps – Keine Weitergabe sensibler Daten an unbefugte Dritte!

Mit zunehmender Sorge beobachtet die Datenschutzkonferenz, dass Betreiber von Gesundheitswebseiten und Gesundheits-Apps auch sensible personenbezogene Daten der Nutzerinnen und Nutzer ohne erkennbare Verarbeitungsgrundlage an Dritte weiterleiten. Unter anderem geschieht dies durch Tracking- und Analyse-Tools (also Programme, die das Surfverhalten beobachten und analysieren), von deren Einsatz die betroffenen Personen keine Kenntnis haben.

So wurde im September 2019 durch die Studie einer Nichtregierungsorganisation bekannt, dass zahlreiche Betreiber von Gesundheitswebseiten, die ihren Besuchern Informationen zu Depression und anderen psychischen Krankheiten anbieten, personenbezogene Nutzungsdaten ohne adäquate Einbindung

der Nutzerinnen und Nutzer an andere Stellen weitergeleitet haben sollen. Teilweise soll dabei sogar die Teilnahme an Depressions-Selbsttests erfasst worden sein. Auch von 44 analysierten deutschen Webseiten besäßen weit über die Hälfte solche integrierten Bausteine, die dies ermöglicht hätten. Im Oktober 2019 wurden Recherchen veröffentlicht, wonach eine in Deutschland ansässige Diagnostik-App ebenfalls Tracking- und Analyse-Dienste nutze und in diesem Zusammenhang sensible Gesundheitsdaten wie z. B. körperliche Beschwerden ohne vorherige Information und Legitimation der Nutzer an Dritte weiterleite.

Zu den Datenempfängern gehören häufig neben sonstigen Tracking-Dienstleistern große Unternehmen wie Facebook, Google und Amazon, die vorrangig eigene Geschäftsinteressen verfolgen. Die Verknüpfung der weitergeleiteten Daten mit anderen Informationen begründet das Risiko, dass für jede Nutzerin und jeden Nutzer ein personenbezogenes Gesundheitsprofil entsteht, von dessen Existenz und Umfang die betroffenen Personen nichts wissen.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder prüfen im Rahmen ihrer Aufgaben und Möglichkeiten derartige Hinweise und werden Datenschutzverletzungen gegebenenfalls sanktionieren. Zugleich ist der Gesetzgeber aufgerufen, im Zusammenhang mit der bevorstehenden Einführung digitaler Gesundheitsanwendungen in die Regelversorgung den Schutz der Vertraulichkeit sensibler Gesundheitsdaten sicherzustellen. Beispielsweise wäre es nicht hinzunehmen, wenn die Nutzung einer von der Regelversorgung erfassten Gesundheits-App zwingend an gesetzlich nicht vorgesehene Weiterleitungen von Gesundheitsdaten gekoppelt würde.

Die Datenschutzkonferenz fordert die Betreiber von Gesundheitswebseiten und Gesundheits-Apps auf, die berechtigten Vertraulichkeitserwartungen ihrer Nutzerinnen und Nutzer zu respektieren. Unabhängig von den allgemeinen datenschutzrechtlichen Anforderungen an die Weitergabe personenbezogener Gesundheitsdaten sind dabei insbesondere folgende Anforderungen zu beachten:

– Leiten Betreiber von Gesundheitswebseiten und Gesundheits-Apps personenbezogene Nutzungsdaten an andere Stellen weiter, sind sie für diese Datenweitergabe verantwortlich, selbst wenn sie – wie etwa bei der Einbindung von Social Plugins – keinen eigenen Zugriff auf die weitergeleiteten Daten haben.
– Als Verantwortliche sind Betreiber insoweit verpflichtet, die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu beachten. Die eingangs beschriebene Weiterleitung von Gesundheitsdaten kann nach Art. 9 Abs. 1, 2 Buchst. a

Datenschutz-Grundverordnung ausnahmsweise nur auf Grundlage einer vor der Datenverarbeitung eingeholten ausdrücklichen Einwilligung zulässig sein, die auch den übrigen Wirksamkeitsvoraussetzungen einer datenschutzrechtlichen Einwilligung genügen muss.

– Insbesondere unterliegt die Einwilligung in die Verarbeitung von Gesundheitsdaten strengen Transparenzanforderungen: Unter anderem muss sie konkret benennen, wer für die Verarbeitung verantwortlich ist und welche Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, Informationen über die sexuelle Orientierung oder zum Sexualleben, verarbeitet werden. Auch die Zwecke der Datenverarbeitung und die Empfänger von weitergeleiteten Daten sind konkret zu benennen. Diese Informationen müssen die Nutzerinnen und Nutzer in die Lage versetzen, sich über die Konsequenzen ihrer erteilten Einwilligung bewusst zu werden.
– Im Rahmen der Regelversorgung wäre die einwilligungsbasierte Weiterleitung von Nutzerdaten an Tracking- oder Analyse-Dienstleister oder sonstige Dritte, die nicht Teil der Gesundheitsversorgung sind, allenfalls zulässig, wenn dies gesetzlich geregelt würde. Gegen eine solche gesetzliche Regelung bestünden allerdings im Hinblick auf das Erfordernis der freiwilligen Einwilligung erhebliche Bedenken.

Im Übrigen weist die Datenschutzkonferenz darauf hin, dass sich aus dem dargestellten Sachverhalt erneut die dringende Notwendigkeit ergibt, möglichst zeitnah eine ePrivacy-Verordnung zu verabschieden. Darin müssen die Bedürfnisse des elektronischen Datenverkehrs mit den Erfordernissen der Grundrechte auf Privatheit und auf Datenschutz in Einklang gebracht werden. Es sind insbesondere Regelungen erforderlich, die einen hohen Schutz sensibler Daten effektiv sicherstellen.

1.8
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06. November 2019

Keine massenhafte automatisierte Aufzeichnung von Kfz-Kennzeichen für Strafverfolgungszwecke!

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist auf den Missstand hin, dass seit einiger Zeit eigentlich für Zwecke der polizeilichen Gefahrenabwehr eingerichtete automatisierte Kennzeichenerfassungssysteme auch für Zwecke der Strafverfolgung eingesetzt werden. Sie erfassen dabei massenhaft und teilweise

längerfristig Kfz-Daten unabhängig von der Beschuldigteneigenschaft der betroffenen Personen.

Im Rahmen der Gefahrenabwehr fahndet die Polizei auf Grundlage des jeweiligen Landespolizeigesetzes nach einzelnen Kraftfahrzeugkennzeichen. Nur im Fall einer Übereinstimmung von Kennzeichen und gesuchtem Fahrzeug kommt es zu einer Speicherung des einzelnen Kraftfahrzeugkennzeichens. Kfz-Kennzeichen, nach denen nicht polizeilich gefahndet wird, werden nach ihrer Erfassung unverzüglich gelöscht.

Demgegenüber wird im Bereich der Strafverfolgung – gestützt auf gerichtliche Beschlüsse oder staatsanwaltliche Anordnungen – nicht nur nach einzelnen Kraftfahrzeugen punktuell gefahndet. Vielmehr werden teilweise zusätzlich die Kennzeichen sämtlicher Fahrzeuge, die eine Straße mit einem Erfassungsgerät passieren, über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert. Als Rechtsgrundlage für solche Strafverfolgungsmaßnahmen wird in der Regel § 100h der Strafprozessordnung (StPO) herangezogen. Dieser erlaubt zwar, zur Observation beschuldigter Personen bestimmte technische Mittel einzusetzen, sofern Gegenstand der Strafverfolgung eine Straftat von erheblicher Bedeutung ist. Gegen andere Personen sind solche Maßnahmen nur ausnahmsweise zulässig. Eine umfassende Datenverarbeitung, wie sie die Aufzeichnung der Kennzeichen aller ein Erfassungsgerät passierenden Kraftfahrzeuge über einen längeren Zeitraum bedeutet, führt jedoch dazu, dass sämtliche Verkehrsteilnehmende im Erfassungsbereich Ziel von Ermittlungsmaßnahmen sind und insoweit Bewegungsprofile entstehen können. Eine Ausweitung des Betroffenenkreises in dieser Größenordnung ist durch keinerlei Tatsachen begründbar und nicht zu rechtfertigen. Sie kann deshalb insbesondere nicht auf § 100h StPO gestützt werden.

Angesichts einer fehlenden Rechtsgrundlage sieht die DSK in der geschilderten exzessiven Nutzung von Kennzeichenerfassungssystemen für die Zwecke der Strafverfolgung einen Verstoß gegen das Grundgesetz und eine Verletzung der Bürgerinnen und Bürger in ihrem Recht auf informationelle Selbstbestimmung. Die DSK fordert die Polizeibehörden und Staatsanwaltschaften auf, die umfassende und unterschiedslose Erfassung, Speicherung und Auswertung von Kraftfahrzeugen durch Kennzeichenerfassungssysteme für Zwecke der Strafverfolgung zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Die DSK lehnt Vorschläge ab, die auf die Schaffung einer neuen Rechtsgrundlage für derartige strafprozessuale Maßnahmen abzielen. Nach verfassungsgerichtlicher Rechtsprechung stellen bereits die automatisierten Kfz-Kennzeichen-Kontrollen zur Fahndung nach Personen oder Sachen

einen Eingriff von erheblichem Gewicht dar, selbst wenn die Kfz-Kennzeichen unverzüglich spurenlos gelöscht werden. Eine längerfristige Aufzeichnung sämtlicher Kennzeichen begründet demgegenüber einen deutlich schwerwiegenderen Grundrechtseingriff.

2. Ausgewählte Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

2.1
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12. September 2019

Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste

Auf Basis des Urteils des EuGH vom 13. Juni 2019 (Az. C – 193/18) zur Auslegung des Begriffs des „Telekommunikationsdienstes“ gelten für die Zuständigkeitsverteilung zwischen dem BfDI und den Aufsichtsbehörden der Länder vorbehaltlich einer Änderung der gesetzlichen Zuständigkeitsregelungen folgende Grundsätze:

1. Webmaildienste sind keine Telekommunikationsdienste i. S. d. Telekommunikationsgesetzes (TKG) in der derzeit geltenden Fassung. Dies gilt für reine Webmaildienste und für E-Maildienste, die zusammen mit einem Internetzugang angeboten werden, wenn die E-Mails (zumindest auch) über einen Webmailer abgerufen werden können. Daraus folgt, dass für die Datenschutzaufsicht mangels anderer besonderer Zuständigkeitsvorschriften allein die jeweiligen Landesdatenschutzaufsichtsbehörden zuständig sind. Die bisher beim Bundesbeauftragten für den Datenschutz (BfDI) geführten Verfahren werden an die jeweils zuständigen Landesaufsichtsbehörden zur Bearbeitung zuständigkeitshalber abgegeben.
2. Messenger-Dienste, die in einem geschlossenen System operieren, d. h. bei denen die Nutzer/innen nur unter sich und nicht mit Nutzer/innen anderer Dienste kommunizieren können, können auch nach der genannten Entscheidung des EuGH als Telekommunikationsdienste i. S. d. TKG angesehen werden mit der Folge, dass für diese Dienste weiterhin der BfDI aufsichtsrechtlich zuständig ist (§ 115 Abs. 4 TKG).

2.2
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12. September 2019

Datenschutzrechtliche Verantwortlichkeit innerhalb der Telematik-Infrastruktur

Die Datenschutzkonferenz vertritt zur Frage der datenschutzrechtlichen Verantwortlichkeit innerhalb der Telematik-Infrastruktur nach § 291a Abs. 7 SGB V folgende Auffassung:

Die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) ist

a. datenschutzrechtlich alleinverantwortlich für die zentrale Zone der TI („TI-Plattform Zone zentral“) sowie
b. „im Sinne des Artikel 26 DSGVO datenschutzrechtlich mitverantwortlich für die dezentrale Zone der TI (‚TI-Plattform Zone dezentral‘). Der Umfang der Verantwortung der gematik für die dezentrale Zone der Telematik-Infrastruktur bedarf einer gesetzlichen Regelung. Die gematik ist verantwortlich für die Verarbeitung, insbesondere soweit sie durch die von ihr vorgegebenen Spezifikationen und Konfigurationen für die Konnektoren, VPN-Zugangsdienste und Kartenterminals bestimmt ist.“

2.3
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[1] – 24. Mai 2019

Asset Deal – Katalog von Fallgruppen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich auf einen Katalog von Fallgruppen verständigt, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f i. V. m. Abs. 4 DS-GVO bei einem Asset Deal zu berücksichtigen sind. Die Fallgruppen lauten:

1. Kundendaten bei laufenden Verträgen

Hier bedarf der Vertragsübergang zivilrechtlich einer Genehmigung der Kundin oder des Kunden (§ 415 BGB / Schuldübernahme). In dieser zivilrechtlichen

1 Unter Ablehnung der Berliner Beauftragten für Datenschutz und Informationsfreiheit sowie des Sächsischen Datenschutzbeauftragten.

Genehmigung wird als Minus auch die datenschutzrechtliche Zustimmung zum Übergang der erforderlichen Daten gesehen. Damit sind die Gegeninteressen der Kundin oder des Kunden gewahrt.

2. Bestandskunden ohne laufende Verträge und letzter Vertragsbeziehung älter als drei Jahre[2]

Daten von Bestandskundinnen und -kunden, bei denen die letzte aktive Vertragsbeziehung mehr als drei Jahre zurückliegt, unterliegen bei einer erwerbenden Stelle einer Einschränkung der Verarbeitung. Diese Daten dürfen zwar übermittelt, aber eben nur wegen gesetzlicher Aufbewahrungsfristen genutzt werden.

Denkbare Alternative ist, dass entsprechende Kundendaten nicht übertragen werden, sondern beim Alt-Unternehmen verbleiben. Ist ein Insolvenzverwalter eingeschaltet, bemüht dieser sich um einen aus der Masse zu finanzierenden Dienstleister, der die Alt-Daten für einen bestimmten Zeitraum aufbewahrt.

3. Daten von Kundinnen und Kunden bei fortgeschrittener Vertragsanbahnung; Bestandskundinnen und -kunden ohne laufende Verträge und letzter Vertragsbeziehung jünger als drei Jahre[3]

Daten solcher Kundinnen und Kunden werden nach Art. 6 Abs. 1 Satz 1 lit. f) DSGVO im Wege der Widerspruchslösung (Opt-out-Modell) mit einer ausreichend bemessenen Widerspruchsfrist (z. B. sechs Wochen) übermittelt. Diese Vorgehensweise ist für die Unternehmen aufwandsschonend und berücksichtigt durch die großzügige Widerspruchsfrist auch die Interessen der Kundinnen und Kunden. Viele Kundinnen und Kunden sind bei einer Aufforderung zu einer ausdrücklichen Einwilligung eher überrascht. Auch sollte darauf geachtet werden, den Widerspruch einfach auszugestalten – z. B. im Online-Verfahren durch Klick auf ein Kästchen.

Die Bankdaten (IBAN) sind jedoch vom Übergang per Widerspruchslösung ausgenommen und nur nach ausdrücklicher Einwilligung des Kunden zu übermitteln.

Darunter fällt nicht das Zahlungsverhalten.

---

2 Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als drei Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

3 Die 3-Jahresfrist berücksichtigt die regelmäßige Anspruchsverjährung. Zudem haben erfahrungsgemäß nichtaktive Kundendaten älter als drei Jahre für die erwerbende Stelle keine Bedeutung mehr und sind veraltet.

4. Kundendaten im Falle offener Forderungen

Die Übertragung offener Forderungen gegen Kundinnen und Kunden richtet sich zivilrechtlich nach den §§ 398 ff. BGB (Forderungsabtretung). In diesem Zusammenhang stehende Daten darf der Zedent (Alt-Gläubiger/Alt-Unternehmen) an den Zessionar (Neu-Gläubiger/Neu-Unternehmen) – gestützt auf Art. 6 Abs. 1 Satz 1 lit. f DS-GVO (früher § 28 Abs. 1 Satz 1 Nr. 2 oder Abs. 2 Nr. 2 lit. a BDSG a. F.) – übermitteln. Überwiegende Gegeninteressen bestehen allerdings dann, wenn die Abtretung durch Vereinbarung ausgeschlossen ist (§ 399 2. Alt. BGB, § 354a HGB).

5. Kundendaten besonderer Kategorie nach Art. 9 Abs. 1 DS-GVO

Solche Daten können nur im Wege der informierten Einwilligung nach Art. 9 Abs. 2 lit. a), Art. 7 DS-GVO übergeleitet werden.

2.4
Beschluss: Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen – 26. April 2019

Zukünftig sollen nach einem Referentenentwurf zur Änderung des Rundfunkbeitragsstaatsvertrags (RBStV) regelmäßig alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt zur Sicherstellung der Aktualität des dortigen Datenbestandes übermittelt werden. Gemäß Art. 1 Ziffer 7 dieses Entwurfs des 23. Rundfunkänderungsstaatsvertrages vom 5. Februar 2019 zählen zu den Meldedaten neben Namen und gegenwärtiger und letzter Anschrift insbesondere auch Geburtstag, Titel, Familienstand sowie die genaue Lage der Wohnung.

Bereits der im Jahr 2013 durchgeführte vollständige Meldedatenabgleich war seinerzeit auf erhebliche datenschutzrechtliche Bedenken gestoßen (vgl. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 11. Oktober 2010). Die DSK stellte ihre Bedenken nur deshalb teilweise zurück, weil lediglich ein einmaliger Meldedatenabgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern. Mit der nun vorgesehenen Regelung wären die – bereits damals zweifelhaften – Zusicherungen des Gesetzgebers, dass es sich bei den anlasslosen vollständigen Meldedatenabgleichen aus den Jahren 2013 und 2018 um einmalige Vorgänge handeln würde, endgültig hinfällig.

Gegen die geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs bestehen weiterhin grundlegende verfassungsrechtliche und datenschutzrechtliche Bedenken.

Ein solcher Abgleich stellt einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung dar und gerät in Konflikt mit den Grundsätzen der Datenminimierung und der Erforderlichkeit gemäß Art. 5 Abs. 1 lit. a und c, Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DSGVO).

Bei einem vollständigen Meldedatenabgleich werden in großem Umfang personenbezogene Daten von Betroffenen, die überhaupt nicht beitragspflichtig sind, weil sie entweder in einer Wohnung leben, für die bereits durch andere Personen Beiträge gezahlt werden oder weil sie von der Beitragspflicht befreit sind, an die Rundfunkanstalten übermittelt und von diesen verarbeitet. Zudem werden auch Daten von all denjenigen Einwohnerinnen und Einwohnern erhoben und verarbeitet, die sich bereits bei der Landesrundfunkanstalt angemeldet haben und regelmäßig ihre Beiträge zahlen. Dabei betrifft der geplante Meldedatenabgleich mehr personenbezogene Daten, als die Beitragszahlerinnen und -zahler bei der Anmeldung mitteilen müssen, z. B. Doktorgrad und Familienstand (vgl. § 8 Abs. 4 RBStV). Es sollen also personenbezogene Daten an die Rundfunkanstalten übermittelt werden, die nicht zur Beitragserhebung notwendig sind.

Die Meldedaten-Übermittlungsverordnungen der Länder bieten mit der anlassbezogenen Meldedatenübermittlung an die Rundfunkanstalten bereits eine angemessene und ausreichende Möglichkeit, die Aktualität des Datenbestandes des Beitragsservices auch bei Veränderungen der Meldesituation der Beitragsschuldnerinnen und Beitragsschuldner zu gewährleisten. Auch wenn die Meldebehörden in Einzelfällen eine Änderungsmitteilung unterlassen sollten, würde ein erneuter vollständiger Meldedatenabgleich in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung der Beitragsschuldner eingreifen, ohne dass dies durch andere Gesichtspunkte, etwa das Ziel der Gebührengerechtigkeit, gerechtfertigt wäre.

Die Landesrundfunkanstalten gehen selbst davon aus, dass ein vollständiger Meldedatenabgleich letztlich in weniger als einem Prozent der Fälle zu einer zusätzlichen, dauerhaften Anmeldung von Beitragspflichtigen führt (vgl. Evaluierungsbericht der Länder gem. § 14 Abs. 9a RBStV vom 20. März 2019).

Die geplanten Regelungen berücksichtigen zudem die Maßstäbe der DS-GVO nicht ausreichend. Nationale Datenschutzvorschriften müssen aufgrund des Anwendungsvorrangs europäischer Verordnungen auf eine Öffnungsklausel der DS-GVO gestützt werden können. Art. 85 Abs. 2 DS-GVO ist nicht einschlägig, da die Datenverarbeitung zum Zweck des Einzugs des Rundfunkbeitrags nicht in dem Anwendungsbereich dieser Norm liegt. Bei Regelungen, die auf die Öffnungsklausel nach Art. 6 Abs. 2 und Abs. 3 i. V. m. Art. 6 Abs. 1 lit. e) DS-GVO gestützt werden, sind die Grundsätze der Datenminimierung und Erforderlichkeit zu beachten. Mitgliedstaatliche

Regelungen für die Erfüllung von Aufgaben, die im öffentlichen Interesse liegen, dürfen danach eingeführt werden, wenn diese die DS-GVO zwar präzisieren, nicht aber deren Grenzen überschreiten. Regelungen, die sich auf diese Öffnungsklausel beziehen, müssen sich folglich in dem Rahmen halten, den die DS-GVO vorgibt. Hier bestehen erhebliche Bedenken im Hinblick auf die Grundsätze der Datenminimierung und der Erforderlichkeit.

Positiv hervorzuheben ist zwar, dass die bisherige Vermieterauskunft im Hinblick auf Mietwohnungen aus § 9 Abs. 1 Satz 2 und 3 RBStV gestrichen werden soll. Ebenso soll der Ankauf von Adressdaten von Privatpersonen ausdrücklich ausgeschlossen werden. Beide Datenverarbeitungen sind aus Sicht des Datenschutzes kritisch zu sehen und ihre Streichung ist zu begrüßen. Dabei darf jedoch nicht übersehen werden, dass mit dem geplanten regelmäßigen vollständigen Meldedatenabgleich eine weitaus umfassendere, datenschutzrechtlich ebenfalls sehr bedenkliche Möglichkeit der Datenerhebung geschaffen werden soll, die das praktische Bedürfnis der Vermieterauskunft und des Ankaufs privater Adressen ohnehin entfallen lässt.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert, den geplanten regelmäßigen vollständigen Meldedatenabgleich nicht einzuführen, da gegen die vorgesehenen Regelungen grundlegende verfassungsrechtliche Bedenken bestehen und diese die Maßstäbe der DS-GVO nicht ausreichend berücksichtigen.

2.5
Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung“ im Erwägungsgrund 33 der DS-GVO – 3. April 2019

Der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ wird in Erwägungsgrund 33 erwähnt, aber in der Datenschutz-Grundverordnung (DSGVO) nicht näher definiert. Er steht in einem engen inhaltlichen Zusammenhang mit der Zweckbestimmung, wie sie bei der Erteilung von Einwilligungen auszugestalten ist. Nach Art. 4 Nr. 11 DSGVO ist eine Einwilligung stets für den „bestimmten Fall“, in informierter Weise und unmissverständlich abzugeben. Das Erfordernis des „bestimmten Falls“ konkretisiert den Grundsatz der Zweckbindung im Sinne des Art. 5 Abs. 1 Buchst. b DSGVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke zu erheben sind.

In ihrem Arbeitspapier 259 rev 01, S. 33, weist die Artikel-29-Datenschutz-Gruppe überdies darauf hin, dass deswegen der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ von dem weit zu verstehenden Begriff der wissenschaftlichen Forschung in Art. 89 DSGVO zu unterscheiden ist. Dort geht es um den Anwendungsbereich der wissenschaftlichen Forschung, nicht um die Zweckbindung im Rahmen einer konkreten Datenverarbeitung. Demgegenüber ist der Begriff „bestimmte Bereiche wissenschaftlicher Forschung“ enger zu verstehen.

Daraus folgt: Nur wenn das konkrete Design des Forschungsvorhabens absehbar bis zum Zeitpunkt der Datenerhebung eine vollständige Zweckbestimmung schlechthin nicht zulässt (vgl. Erwägungsgrund 33, Satz 1), kann beispielsweise der Ansatz der breiten Einwilligung (broad consent) zum Tragen kommen. Bei der einer Datenerhebung zeitlich vorgelagerten Einwilligung können dann unter engen Voraussetzungen Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden.

Auch der Erwägungsgrund 33 entbindet allerdings nicht von der Pflicht, im Kontext von Forschungsprojekten Mechanismen herauszuarbeiten, nach denen die Verwendung der erhobenen Daten für die betroffene Person nachvollziehbar eingegrenzt wird. Insbesondere wird es nicht als mit dem Erwägungsgrund 33 vereinbar erachtet, wenn die Verwendung der erhobenen Daten pauschal auf bestimmte Forschungsbereiche ausgeweitet wird. Das Gebot einer informierten Einwilligung erfordert zumindest, dass möglichst präzise das jeweilige Forschungsvorhaben und nachfolgend aufgeführte spezifische Sicherungsmaßnahmen von der Einwilligungserklärung erfasst werden.

In den Einzelfällen, in denen das Arbeiten mit breiten Einwilligungen als für das Erreichen des Forschungszwecks zwingend erforderlich erachtet wird, ist deshalb insbesondere mit den folgenden Korrektiven zu arbeiten. Sie dienen der Transparenz, Vertrauensbildung und Datensicherheit, um die abstraktere Fassung des Forschungszwecks zu kompensieren:

A. Zusätzliche Sicherungsmaßnahmen zur Gewährleistung von Transparenz

– Verwendung einer für den Einwilligenden zugänglichen Nutzungsordnung oder eines einsehbaren Forschungsplanes, der die geplanten Arbeitsmethoden und die Fragen, die Gegenstand der Forschung sein sollen, beleuchtet

– Ausarbeitung und Dokumentation im Hinblick auf das konkrete Forschungsprojekt, wieso in diesem Fall eine nähere Konkretisierung der Forschungszwecke nicht möglich ist
– Einrichten einer Internetpräsenz, durch die die Studienteilnehmer über laufende und künftige Studien informiert werden

B. Zusätzliche Sicherungsmaßnahmen zur Vertrauensbildung

– positives Votum eines Ethikgremiums vor der Nutzung für weitere Forschungszwecke
– Prüfung, ob das Arbeiten mit einem dynamic consent möglich ist bzw. Einräumung einer Widerspruchsmöglichkeit vor der Verwendung der Daten für neue Forschungsfragen

C. Zusätzliche Garantiemaßnahmen zur Datensicherheit

Verstärkter Einsatz von Garantien im Hinblick auf die erhobenen Daten durch technisch-organisatorische Maßnahmen wie:

– keine Datenweitergabe in Drittländer mit geringerem Datenschutzniveau
– gesonderte Zusagen zur Datenminimierung, Verschlüsselung, Anonymisierung oder Pseudonymisierung
– spezifische Vorschriften für die Begrenzung des Zugriffs auf die erhobenen Daten

Das Ergebnis der Prüfung einschließlich der zugrundeliegenden Beweggründe sowie die Sicherstellung der o. g. Sicherungsmaßnahmen sind zu dokumentieren und den zur Prüfung der ethischen und datenschutzrechtlichen Vereinbarkeit des Forschungsvorhabens zuständigen Stellen zusammen mit dem Forschungskonzept vorzulegen.

2.6
Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit[4] – 01.04.2019

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich am 5. September 2018 zu dem (Weiter-) Betrieb von Facebook-Fanpages nach dem Urteil des EuGH vom 5. Juni 2018 geäußert. In ihrem Beschluss hat die Konferenz deutlich gemacht, dass Fanpage-Betreiber die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO nachweisen können müssen. Dies ergibt sich aus der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO sowie insbesondere in Bezug auf Verpflichtungen nach Art. 24, 25, 32 DSGVO.

Am 11. September 2018 veröffentlichte Facebook eine sog. „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ sowie „Informationen zu Seiten-Insights“. Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO. Insbesondere steht es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DSGVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten“ einräumen lassen will. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar. Sie sind nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen. Vor diesem Hintergrund bekräftigt die Konferenz erneut die Rechenschaftspflicht der Fanpage-Betreiber (unabhängig von dem Grad der Verantwortlichkeit) und stellt fest:

1. Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO und – soweit besondere Kategorien personenbezogener Daten verarbeitet werden – nach Art. 9 Abs. 2 DSGVO. Dies gilt auch in den Fällen, in denen sie die Verarbeitungstätigkeiten nicht unmittelbar selbst

4 Unter Enthaltung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit.

durchführen, sondern durch andere gemeinsam mit ihnen Verantwortlichen durchführen lassen.

2. Ohne hinreichende Kenntnis über die Verarbeitungstätigkeiten, die der eigenen Verantwortung unterliegen, sind Verantwortliche nicht in der Lage zu bewerten, ob die Verarbeitungstätigkeiten rechtskonform durchgeführt werden. Bestehen Zweifel, geht dies zulasten der Verantwortlichen, die es in der Hand haben, solche Verarbeitungen zu unterlassen. Der EuGH führt hierzu aus: „Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien." (EuGH, C-210/16, Rn. 40)
3. Im Hinblick auf die Ausführungen zur „Hauptniederlassung für die Verarbeitung von Insights-Daten für sämtliche Verantwortliche" sowie zur federführenden Aufsichtsbehörde (Punkt 4 in der „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen") weist die Konferenz darauf hin, dass sich die Zuständigkeit der jeweiligen Aufsichtsbehörden für Fanpage-Betreiber nach der DSGVO richtet. Nach Art. 55 ff. DSGVO sind die Aufsichtsbehörden für Verantwortliche (wie z. B. Fanpage-Betreiber) in ihrem Hoheitsgebiet zuständig. Dies gilt unabhängig von den durch die DSGVO vorgesehenen Kooperations- und Kohärenzmechanismen.

Sowohl Facebook als auch die Fanpage-Betreiber müssen ihrer Rechenschaftspflicht nachkommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen wird, ist ein datenschutzkonformer Betrieb einer Fanpage nicht möglich.

3. Ausgewählte Orientierungshilfen, Positionspapiere und sonstige Veröffentlichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

3.1

Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen – 14. Oktober 2019

I.
Einleitung

Am 25. Mai 2018 hat der Europäische Datenschutzausschuss (EDSA) in seiner ersten Plenarsitzung entsprechend seiner Aufgabe in Art. 70 Abs. 1 Buchst. k) DS-GVO die Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 der Artikel-29-Datenschutzgruppe vom 03.10.2017 (WP 253) bestätigt. Diese legen insbesondere die einheitliche Auslegung der Bestimmungen von Art. 83 DS-GVO fest und umreißen ein einheitliches Konzept zu den Grundsätzen bei der Festsetzung von Geldbußen. Die Leitlinien sind jedoch nicht erschöpfend und die Konkretisierung der Festsetzungsmethodik bleibt späteren Leitlinien des EDSA vorbehalten.

Das Konzept betrifft die Bußgeldzumessung in Verfahren gegen Unternehmen im Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO). Es findet insbesondere keine Anwendung auf Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit. Das Konzept ist auch weder für grenzüberschreitende Fälle noch für andere Datenschutzaufsichtsbehörden der EU bindend. Ferner entfaltet es keine Bindung hinsichtlich der Festlegung von Geldbußen durch Gerichte.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder können jederzeit eine Aufhebung, Änderung oder Erweiterung ihres Konzepts mit Wirkung für die Zukunft beschließen. Das Konzept verliert zudem seine Gültigkeit, sobald der EDSA seine abschließenden Leitlinien zur Methodik der Festsetzung von Geldbußen erlassen hat.

II.
Bußgeldkonzept

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sind der Auffassung, dass in einem modernen Unternehmenssanktionsrecht

mit erheblichen maximalen Bußgeldbeträgen, das sich zugleich an eine Vielfalt unterschiedlich großer Unternehmen richtet, der Umsatz eines Unternehmens eine geeignete, sachgerechte und faire Anknüpfung zur Sicherstellung der Wirksamkeit, Verhältnismäßigkeit und Abschreckung darstellt.

Vor diesem Hintergrund erfolgt die Bußgeldzumessung in Verfahren gegen Unternehmen in fünf Schritten. Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.).

Dieses Verfahren garantiert eine nachvollziehbare, transparente und einzelfallgerechte Form der Bußgeldzumessung.

1. Kategorisierung der Unternehmen nach Größenklassen

Das betroffene Unternehmen wird anhand seiner Größe einer von vier Größenklassen (A bis D) zugeordnet (Tabelle 1).

Die Größenklassen richten sich nach dem gesamten weltweit erzielten Vorjahresumsatz der Unternehmen (vgl. Art. 83 Abs. 4 bis 6 DS-GVO) und sind unterteilt in Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) sowie Großunternehmen. Es gilt gemäß dem Erwägungsgrund 150 der DS-GVO der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV (sog. funktionaler Unternehmensbegriff).

Die Größeneinordnung der KMU orientiert sich hinsichtlich des Vorjahresumsatzes grundsätzlich an der Empfehlung der Kommission vom 6. Mai 2003 (2003/361/EG).

Die Größenklassen werden zur konkreteren Einordnung der Unternehmen nochmals in Untergruppen unterteilt (A.I bis A.III, B.I bis B.III, C.I bis C.VII, D.I bis D.VII).

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)						**Großunternehmen**	
A		**B**		**C**		**D**	
Kleinst-unternehmen: Jahresumsatz bis 2 Mio. €		**Kleine Unternehmen:** Jahresumsatz über 2 Mio. € bis 10 Mio. €		**Mittlere Unternehmen:** Jahresumsatz über 10 Mio. € bis 50 Mio. €		Jahresumsatz über 50 Mio €	
A.I	Jahresumsatz bis 700.000 €	**B.I**	Jahresumsatz über 2 Mio. € bis 5 Mio. €	**C.I**	Jahresumsatz über 10 Mio. € bis 12,5 Mio. €	**D.I**	Jahresumsatz über 50 Mio. € bis 75 Mio. €
A.II	Jahresumsatz über 700.000 € bis 1,4 Mio. €	**B.II**	Jahresumsatz über 5 Mio. € bis 7,5 Mio. €	**C.II**	Jahresumsatz über 12,5 Mio. € bis 15 Mio. €	**D.II**	Jahresumsatz über 75 Mio. € bis 100 Mio. €
A.III	Jahresumsatz über 1,4 Mio. € bis 2 Mio. €	**B.III**	Jahresumsatz über 7,5 Mio. € bis 10 Mio. €	**C.III**	Jahresumsatz über 15 Mio. € bis 20 Mio. €	**D.III**	Jahresumsatz über 100 Mio. € bis 200 Mio. €
				C.IV	Jahresumsatz über 20 Mio. € bis 25 Mio. €	**D.IV**	Jahresumsatz über 200 Mio. € bis 300 Mio. €
				C.V	Jahresumsatz über 25 Mio. € bis 30 Mio. €	**D.V**	Jahresumsatz über 300 Mio. € bis 400 Mio. €
				C.VI	Jahresumsatz über 30 Mio. € bis 40 Mio. €	**D.VI**	Jahresumsatz über 400 Mio. € bis 500 Mio. €
				C.VII	Jahresumsatz über 40 Mio. € bis 50 Mio. €	**D.VII**	Jahresumsatz über 500 Mio. €

(Tabelle 1)

2. Bestimmung des mittleren Jahresumsatzes der jeweiligen Untergruppe der Größenklasse

Dann wird der mittlere Jahresumsatz der Untergruppe, in die das Unternehmen eingeordnet wurde, bestimmt (Tabelle 2). Dieser Schritt dient der Veranschaulichung der darauf aufbauenden Ermittlung des wirtschaftlichen Grundwertes (3.).

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)							**Groß-unternehmen**
A		**B**		**C**			**D**
A.I	350.000 €	**B.I**	3,5 Mio. €	**C.I**	11,25 Mio. €	**D.I**	62,5 Mio. €
A.II	1.050.000 €	**B.II**	6,25 Mio. €	**C.II**	13,75 Mio. €	**D.II**	87,5 Mio. €
A.III	1,7 Mio. €	**B.III**	8,75 Mio. €	**C.III**	17,5 Mio. €	**D.III**	150 Mio. €
				C.IV	22,5 Mio. €	**D.IV**	250 Mio. €
				C.V	27,5 Mio. €	**D.V**	350 Mio. €
				C.VI	35 Mio. €	**D.VI**	450 Mio. €
				C.VII	45 Mio. €	**D.VII**	konkreter Jahresumsatz*

(Tabelle 2)

* Ab einem jährlichen Umsatz von über 500 Mio. € ist der prozentuale Bußgeldrahmen von 2 % bzw. 4 % des jährlichen Umsatzes als Höchstgrenze zugrunde zu legen, so dass beim jeweiligen Unternehmen eine Berechnung anhand des konkreten Umsatzes erfolgt.

3. Ermittlung des wirtschaftlichen Grundwertes

Für die Festsetzung des wirtschaftlichen Grundwertes wird der mittlere Jahresumsatz der Untergruppe, in die das Unternehmen eingeordnet wurde, durch 360 (Tage) geteilt und so ein durchschnittlicher, auf die Vorkommastelle aufgerundeter Tagessatz errechnet (Tabelle 3).

Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)						Großunternehmen	
A		B		C		D	
A.I	972 €	**B.I**	9.722 €	**C.I**	31.250 €	**D.I**	173.611 €
A.II	2.917 €	**B.II**	17.361 €	**C.II**	38.194 €	**D.II**	243.056 €
A.III	4.722 €	**B.III**	24.306 €	**C.III**	48.611 €	**D.III**	416.667 €
				C.IV	62.500 €	**D.IV**	694.444 €
				C.V	76.389 €	**D.V**	972.222 €
				C.VI	97.222 €	**D.VI**	1,25 Mio. €
				C.VII	125.000 €	**D.VII**	konkreter Tagessatz*

(Tabelle 3)

* Ab einem jährlichen Umsatz von über 500 Mio. € ist der prozentuale Bußgeldrahmen von 2 % bzw. 4 % des jährlichen Umsatzes als Höchstgrenze zugrunde zu legen, so dass beim jeweiligen Unternehmen eine Berechnung anhand des konkreten Umsatzes erfolgt.

4. Multiplikation des Grundwertes nach Schweregrad der Tat

Danach erfolgt anhand der konkreten tatbezogenen Umstände des Einzelfalls (vgl. Art. 83 Abs. 2 Satz 2 DS-GVO) eine Einordnung des Schweregrads der Tat in leicht, mittel, schwer oder sehr schwer.

Hierfür werden gemäß der nachstehenden Tabelle 4 unter Berücksichtigung der Umstände des Einzelfalls anhand des Kriterienkatalogs des Art. 83 Abs. 2 DS-GVO der Schweregrad des Tatvorwurfs und der jeweilige Faktor ermittelt, mit dem der Grundwert multipliziert wird. Im Hinblick auf die unterschiedlichen Bußgeldrahmen sind dabei für formelle (Art. 83 Abs. 4 DS-GVO) und materielle (Art. 83 Abs. 5, 6 DS-GVO) Verstöße jeweils unterschiedliche Faktoren zu wählen. Bei der Wahl des Multiplikationsfaktors einer sehr schweren Tat ist zu beachten, dass der einzelfallbezogene Bußgeldrahmen nicht überschritten wird.

Schweregrad der Tat	Faktor für formelle Verstöße gemäß Art. 83 Abs. 4 DS-GVO	Faktor für materielle Verstöße gemäß § 83 Abs. 5, 6 DS-GVO
Leicht	1 bis 2	1 bis 4
Mittel	2 bis 4	4 bis 8
Schwer	4 bis 6	8 bis 12
Sehr Schwer	6 <	12 <

(Tabelle 4)

5. Anpassung des Grundwertes anhand aller sonstigen für und gegen den Betroffenen sprechenden Umstände

Der unter 4. errechnete Betrag wird anhand aller für und gegen den Betroffenen sprechenden Umstände angepasst, soweit diese noch nicht unter 4. berücksichtigt wurden. Hierzu zählen insbesondere sämtliche täterbezogenen Umstände (vgl. Kriterienkatalog des Art. 83 Abs. 2 DSGVO) sowie sonstige Umstände, wie z. B. eine lange Verfahrensdauer oder eine drohende Zahlungsunfähigkeit des Unternehmens.

3.2
Orientierungshilfe zur Videoüberwachung in Schwimmbädern – 08. Januar 2019

Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises vom 19.02.2014

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen. Ansonsten ist die Datenschutz-Grundverordnung (DS-GVO) anwendbar.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Die Verarbeitung personenbezogener Daten ist rechtmäßig, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und 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. Da sich die

Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten und sich demgemäß ungezwungen verhalten möchten sowie zudem nur leicht bekleidet sind, genießen sie besonderen Schutz. Die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf daher besonderer Sorgfalt. Zudem sind eine Vielzahl der Schwimmbadbesucher Kinder, die ebenfalls von der Videoüberwachung erfasst werden. Ihr Interesse ist im Rahmen der Interessenabwägung entsprechend der gesetzlichen Vorgaben besonders zu gewichten. Bei der Abwägung sind auch die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen (Erwägungsgrund 47 DS-GVO). Besucher erwarten im Rahmen eines Schwimmbadbesuches jedenfalls in den meisten Bereichen eines Schwimmbades nicht, von Videokameras erfasst zu werden.

Unabhängig von der Frage eines berechtigten Interesses ist eine Videoüberwachung jedenfalls in der Regel nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann in der Regel durch andere geeignete Maßnahmen, wie etwa ausreichend hohe Drehkreuze oder Schranken, ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auch auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung in der Regel außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen unzulässig. Es ist nach Art. 8 der Charta der Grundrechte der Europäischen Union nicht verhältnismäßig, einen derartigen Eingriff in die Interessen und das Recht auf Schutz der personenbezogenen Daten einer

Person für eine große Zahl von Personen hinzunehmen, nur damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Zudem wird zumeist eine große Anzahl von Kindern erfasst, deren Interessen und Grundrechte von der DS-GVO in besonderem Maße geschützt werden. Ein solcher Eingriff in deren Interessen und Grundrechte ist daher nicht gerechtfertigt. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen.[1]

Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen immer, wenn die Intimsphäre der betroffenen Person berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z. B. Beschädigung von Haartrocknern).

Darüber hinaus sind ggf. weitere datenschutzrechtliche Voraussetzungen (z. B. Verzeichnis von Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

1 OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch – wenn auch nicht ununterbrochen – auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

3.3
Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen – 16. Januar 2019

Aufgrund der immer erschwinglicheren Preise werden Drohnen immer häufiger für die Freizeitgestaltung gekauft und von nicht-öffentlichen Stellen im nachbarschaftlichen Umfeld oder für gewerbliche Zwecke eingesetzt.

Sind die Drohnen mit Kameras ausgestattet, ermöglichen sie unbeobachtete Blicke in nicht einfach zugängliche Orte wie den Garten oder auf die Sonnenterrasse des Nachbarn, aber auch auf öffentliche Straßen oder Plätze. Dabei handelt es sich um eine Datenverarbeitung mittels Videoüberwachung. Der potenziell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar.

Allerdings ist beim Einsatz von Drohnen die Luftverkehrs-Verordnung (LuftVO) zu beachten. Diese enthält ein Verbot zum Betrieb unbemannter Luftfahrtsysteme und Flugmodelle an bestimmten Orten.

Nach § 21b Abs. 1 Ziff. 2 der LuftVO ist der Betrieb von Drohnen u. a. über und in einem seitlichen Abstand von 100 Metern von Menschenansammlungen, Unglücksorten, Katastrophengebieten und anderen Einsatzorten von Behörden und Organisationen mit Sicherheitsaufgaben verboten. Zudem ist nach Ziff. 7 der gleichen Vorschrift u. a. auch der Betrieb von Drohnen, die elektronische Bildaufnahmen anfertigen können, über Wohngrundstücken verboten, wenn der betroffene Eigentümer oder sonstige Nutzungsberechtigte nicht ausdrücklich zugestimmt hat. Dadurch wird der zulässige örtliche Einsatzbereich von Kameradrohnen durch nicht-öffentliche Stellen von vornherein eingeschränkt.

Zudem muss sich der Einsatz an den datenschutzrechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) messen lassen, sobald eine Datenverarbeitung nicht ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten erfolgt, sondern z. B. zu gewerblichen Zwecken oder zum Zwecke der Veröffentlichung.

So bedarf es für die Verarbeitung einer Rechtsgrundlage. Beispielsweise muss die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich sein und demgegenüber dürfen schutzbedürftige Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Absatz 1 Satz 1 Buchstabe f DS-GVO). Das be-

deutet, die Interessen des Verantwortlichen, der eine Drohne einsetzt, sind mit den Interessen der davon Betroffenen abzuwägen. Eine entscheidende Rolle spielt dabei jeweils der Einsatzzweck. Die genannten Voraussetzungen sind in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht erfüllt. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet erstellt werden.

Darüber hinaus ist zu bedenken, dass es für Betroffene auch nicht ohne weiteres möglich ist, den für den Drohneneinsatz Verantwortlichen zu erkennen. Zudem können die für die Verarbeitung personenbezogener Daten erforderlichen Informationspflichten gem. Art. 12 ff. DS-GVO in der Regel nicht erfüllt werden. Aus diesen Gründen kann der Einsatz von Drohnen, die mit Videokameras ausgerüstet sind, im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen bei der Erfassung personenbezogener Daten mit einem ungleich größeren Eingriff in das Recht auf Schutz der personenbezogenen Daten der Betroffenen (Art. 8 der Charta der Grundrechte der Europäischen Union) verbunden sein.

Wenn Drohnen mit Kameras innerhalb des Anwendungsbereiches der DS-GVO betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Aufsichtsbehörde hierfür ein Bußgeld verhängen.

Neben dem aufsichtsbehördlichen Verfahren steht Betroffenen auch der Zivilrechtsweg offen. Bei einem Grundrechtseingriff kann u. U. ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Absatz 1 des Bürgerlichen Gesetzbuches (BGB) geltend gemacht werden. Auch die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche mithin Bereiche der Intimsphäre (§ 201a des Strafgesetzbuches (StGB)) oder der Aufzeichnung des nicht-öffentlich gesprochenen Wortes (§ 201 StGB).

Drohnenbetreiber sind daher aufgefordert, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann. Insbesondere in urbanen Umgebungen ist das Betreiben von Drohnen mit Film- und Videotechnik im Einklang mit den geltenden Gesetzen in der Regel nicht möglich.

3.4
Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams) – 28. Januar 2019

Dashcams werden auch in Deutschland in immer mehr Fahrzeugen eingesetzt, zumeist um im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können. Dabei wird üblicherweise das gesamte Umfeld aufgenommen, ohne dass eine Verpixelung von Personen oder Kennzeichen anderer Fahrzeuge erfolgt.

Der Einsatz solcher Kameras ist datenschutzrechtlich kaum zulässig.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Verwendung von Filmaufnahmen zur Dokumentation eines etwaigen Unfallhergangs angegeben wird, ist der Einsatz – auch wenn die Kameras von Privatpersonen eingesetzt werden – an Art. 6 Absatz 1 Satz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) zu messen. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Das bedeutet, die Interessen des Verantwortlichen, der eine Dashcam einsetzt, sind mit den Interessen der davon Betroffenen abzuwägen. Eine entscheidende Rolle spielt dabei jeweils der Einsatzzweck.

Die genannten Voraussetzungen sind jedenfalls bei einer permanenten anlasslosen Aufzeichnung des Verkehrsgeschehens nicht erfüllt, da diese Betriebsform zur Wahrung der Beweissicherungsinteressen nicht erforderlich ist und die schutzwürdigen Interessen betroffener Personen, zumeist unbeteiligter Verkehrsteilnehmer, überwiegen. Letztere können sich insbesondere auf ihr Grundrecht aus Art. 8 der Charta der Grundrechte der Europäischen Union berufen. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dies umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Dauerhaft aufzeichnende Dashcams erheben permanent und ohne Anlass personenbezogene Daten, wie Kennzeichen der anderen Verkehrsteilnehmer oder Personen, die sich in der Nähe einer Straße aufhalten, so dass eine Vielzahl von Verkehrsteilnehmern von der Verarbeitung personenbezogener Daten betroffen ist, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers als datenschutzrechtlich Verantwortlicher, für den Fall eines Verkehrsunfalls

Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Recht auf Schutz der personenbezogenen Daten der anderen Verkehrsteilnehmer nicht rechtfertigen.

Zudem muss auch bei einer Videoüberwachung mittels Dashcam der Verantwortliche sicherstellen, dass er die betroffenen Personen gemäß Art. 12 ff DS-GVO auf die kameragestützte Verarbeitung personenbezogener Daten transparent hinweist, auch wenn dies gerade bei fahrenden Fahrzeugen in praktischer Hinsicht Schwierigkeiten aufwirft.

Auch wenn der Bundesgerichtshof in der Entscheidung vom 15. Mai 2018 – VI ZR 233/17 – eine Beweisverwertbarkeit von Aufnahmen im Zivilprozess nicht verneint, betont er gleichzeitig, dass der anlasslose Einsatz von dauerhaft aufzeichnenden Dashcams datenschutzrechtlich unzulässig ist. Eine Ausnahme kann danach überhaupt nur in Betracht kommen, wenn (technische) Möglichkeiten zum Einsatz gebracht werden, die sicherstellen, dass eine Kamera lediglich kurzzeitig anlassbezogen aufzeichnet. Auch hier sind die Informationspflichten nach Art. 12 ff. DS-GVO zu berücksichtigen.

Folglich können die Aufsichtsbehörden – unabhängig von der Verwertbarkeit im Zivilprozess – Verbote aussprechen und empfindliche Bußgelder verhängen. Diese Bußgelder können den finanziellen Vorteil, der in einem Zivilprozess erstritten wird, unter Umständen wieder aufheben.

3.5
Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen – 22. Februar 2019

I.
Vorwort

Auch private Sicherheitsunternehmen rüsten ihre Beschäftigten mittlerweile mit Bodycams aus. Als Gründe führen sie z. B. Schutz der Beschäftigten vor Übergriffen, Beschaffung von Beweismitteln für zivilrechtliche Ansprüche oder eine abschreckende bzw. deeskalierende Wirkung an. Dem Einsatz von Bodycams stehen allerdings datenschutzrechtliche Bedenken entgegen.

II.
Eingriff in Persönlichkeitsrechte

Das Aufzeichnen von Bild und Ton mittels einer Bodycam greift in die Persönlichkeitsrechte Betroffener ein und ist rechtfertigungsbedürftig. Für unbeteiligte Dritte ist nicht ohne weiteres erkennbar, ob eine Bodycam Bild und Ton aufzeichnet, weshalb die Möglichkeit besteht, dass die bloße Anwesenheit dieses Geräts auf sie einschüchternd wirkt. Der Einsatz an kommunikativen Orten birgt die Gefahr, dass Anwesende von ihren Grundrechten, wie beispielsweise der Meinungsfreiheit, nur eingeschränkt Gebrauch machen. Wenn mit Bodycams ausgerüstete Sicherheitskräfte Streifengänge auf einem gut besuchten Gelände unternehmen oder eine Menschenmenge durchqueren, können Anwesende unvermittelt in das unmittelbare Blickfeld der Geräte gelangen, so dass sie detaillierte Film- oder sogar Tonaufnahmen befürchten müssen. Je nach Befestigung und Verwendung der Bodycam kann es auch zu einer unbemerkten, und damit heimlichen, Videoüberwachung kommen.

Dadurch, dass sich der Blickwinkel der Bodycam ständig ändert, kann es zu einer umfangreichen Erfassung der Umgebung einschließlich geschützter Bereiche wie Sanitäranlagen oder ständiger Arbeitsplätze von Beschäftigten kommen. Wenn bereits eine Videoüberwachung mittels statischer Kameras eingerichtet ist, kann dies zusammen mit mobilen Geräten zu einer nahezu lückenlosen Überwachung führen.

Der Eingriff ist für diejenigen besonders schwerwiegend, die auf die Benutzung bestimmter Orte angewiesen sind. Auch die Trägerinnen und Träger selbst können durch die Bodycams beeinträchtigt werden: Sie nehmen während der Beobachtung zugleich ihr eigenes Verhalten auf.

III.
Datenschutzgerechter Einsatz

Ein datenschutzgerechter Einsatz der Bodycam ist an Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DS-GVO), § 4 Bundesdatenschutzgesetz (BDSG) zu messen. Danach ist die Verarbeitung personenbezogener Daten zulässig, soweit sie für die Wahrnehmung des Hausrechts oder die Wahrung berechtigter Interessen (*1.*) von Verantwortlichen oder Dritten geeignet (*2.*) und erforderlich (*3.*) ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (*4.*).

1. Berechtigtes Interesse / Zweck der Verarbeitung

Vor Inbetriebnahme muss eindeutig festgelegt sein, welches berechtigte Interesse bzw. welcher Zweck mit dem Einsatz einer Bodycam verfolgt werden soll. In Betracht kommt u. a. der Schutz des eigenen Personals vor Übergriffen, die nachträgliche Identifikation eines Tatverdächtigen und die Sicherung von Beweismitteln für die Verfolgung zivilrechtlicher Ansprüche. Die Unterstützung bei der Strafverfolgung stellt kein eigenes berechtigtes Interesse für die Einführung von Bodycams dar. Die Abwehr von Gefahren und die Beseitigung von Störungen der öffentlichen Sicherheit und Ordnung ist Aufgabe der Polizei; die Verfolgung von Straftaten obliegt den Strafverfolgungsbehörden. Der Zweck, ein subjektives Sicherheitsgefühl der Bürgerinnen und Bürgern zu steigern, reicht allein nicht aus, einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Videoüberwachung sollte kein trügerisches Gefühl von Sicherheit vermitteln, wo objektiv die Sicherheit nicht erhöht wird.

Der Einsatz von Bodycams kann nur zulässig sein, wenn er anlassbezogen zu Zwecken erfolgt, die im Vorhinein eindeutig festgelegt sind. Um einen zweckgebundenen Einsatz der Kameras sicherzustellen, ist vor der erstmaligen Inbetriebnahme ein Einsatzkonzept zu erstellen. Das Einsatzkonzept kann Teil einer Dienst- oder Betriebsvereinbarung sein. Darin ist abschließend festzulegen, in welchen Situationen die Kameras konkret eingesetzt werden sollen und welches Verfahren dabei beachtet werden muss.

Der Einsatz von Bodycams ist beispielsweise in Situationen möglich, bei der eine Person aggressives Verhalten (körperliche Auseinandersetzung, Drohungen, Beleidigungen etc.) zeigt oder eine Situation unmittelbar zu eskalieren droht. Nicht aggressives, passives oder nicht gewalttätiges Verhalten einer Person berechtigt dagegen grundsätzlich nicht zu einem Kameraeinsatz. Festzulegen ist auch, in welchen Räumen mit einer Bodycam gefilmt werden darf. Die Aufnahme sensibler Bereiche wie Toiletten, Sanitärräume, Umkleidebereiche, Pausen- oder Aufenthaltsräume ist auszuschließen. Um Überwachungsdruck in der Öffentlichkeit zu vermeiden, kann der Verantwortliche den Einsatz der Kameras auf Flächen beschränken, in welchen das Hausrecht auszuüben er berechtigt. Um nachweisen zu können, dass ein Einsatz der Bodycam rechtmäßig erfolgt ist, sollte jeder Vorfall im Nachhinein ausreichend dokumentiert sein; mindestens mit dem jeweiligen Anlass, dem Zeitpunkt und den beteiligten Personen. Technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten sind in das Konzept aufzunehmen.

2. Bodycam zur Zweckerreichung geeignet?

Es muss sich objektiv begründen lassen, dass der Einsatz der Bodycams zum Erreichen des Zwecks geeignet ist. Dafür ist zu fragen, ob sich der festgelegte Zweck durch die Verwendung solcher Geräte an dem jeweiligen Einsatzort und zu den jeweiligen äußeren Einsatzbedingungen tatsächlich erreichen lässt. Es ist zweifelhaft, ob das Mitführen einer Bodycam durch eine subjektiv mögliche Abschreckungswirkung wirksam verhindern kann, dass sich eine Straftat ereignet. Berücksichtigt werden muss auch eine mögliche Provokationswirkung durch die Bodycam. Außerdem können Aufzeichnungen einer Bodycam immer nur die Sicht der Trägerin bzw. des Trägers wiedergeben, weshalb der Aufklärungswert dieser Aufnahmen in besonders unübersichtlichen und schnelllebigen Situationen zweifelhaft ist. Damit eignet sich die Bodycam grundsätzlich nicht in jedem Fall zum Zweck der Aufklärung von Vorfällen.

3. Bodycam zur Zweckerreichung erforderlich?

Außerdem ist zu prüfen, ob nicht gleichwirksame Mittel zur Verfügung stehen, die weniger in die Persönlichkeitsrechte Betroffener eingreifen. In Betracht kommt hierbei, die Anzahl des Sicherheitspersonals pro Streife zu erhöhen, die Beleuchtung auszuweiten, Notfall- oder Alarmknöpfe zu installieren oder Sicherheitskräfte mit Funksprechgeräten auszustatten, damit diese im Konfliktfall weiteres Personal herbeirufen können. Eine dauerhafte und anlasslose Aufnahme ist zur Zweckerreichung in der Regel nicht erforderlich und muss ausgeschlossen sein.

4. Interessenabwägung – Schutzmaßnahmen

Ergibt die Prüfung, dass der Bodycameinsatz im o. g. Sinne geeignet und erforderlich ist, sind die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen mit den berechtigten Interessen des Verantwortlichen abzuwägen.

Da der Einsatz von Bodycams aus den eingangs benannten Gründen für die betroffenen Personen einen tiefen Eingriff in ihre Grundrechte und Grundfreiheiten bedeutet, dürfte er allenfalls dann in Betracht kommen, wenn die Interessenabwägung zu Gunsten der Verantwortlichen ausfällt. Dies ist der Fall, wenn mindestens die folgenden Maßnahmen getroffen werden, um den schutzwürdigen Interessen der Betroffenen Rechnung zu tragen:

– Im konkreten Einsatz (s. o.) darf die Bodycam nur dann aktiviert werden, wenn ein entsprechender Vorfall zu erwarten ist. Die Zielperson muss vor dem Einschalten der Bodycam auf die Aufnahme hingewiesen werden.

Sollte sich die Situation bereits dadurch entschärfen, darf die Bodycam nicht aktiviert werden. Ein Dauerbetrieb ist unzulässig. Vorfälle sind zu dokumentieren.

– Bei Aktivierung der Bodycam muss ein optisches Signal aktiviert werden („rote Lampe“), welches anzeigt, ob das Gerät Daten erhebt. Zudem sollten Sicherheitskräfte mit Bodycams entsprechend gekennzeichnet sein, etwa durch beschriftete Warnwesten mit Kamerasymbolen.
– Sollte es zu einer Datenerhebung kommen, ist dies hinreichend transparent zu machen (Art. 5 Abs. 1 DS-GVO). Dabei sind die Vorgaben des Art. 12 ff. DS-GVO zu beachten (vgl. unten).
– Eine Pre-Recording-Funktion darf nur anlassbezogen eingesetzt werden. Im Einsatzkonzept muss hierzu festgelegt sein, dass ein Pre-Recording nur bei einer drohenden Gefahr oder einer Situation aktiviert werden darf, bei der ein gewisses Gefahrenpotenzial besteht, das Sicherheitspersonal aber noch nicht unmittelbar eingreifen muss. Die Aktivierung der Pre-Recording-Funktion muss durch das Sicherheitspersonal angekündigt werden. Nach 60 Sekunden sind die Aufnahmen des Pre-Recording automatisiert zu löschen und dabei in einem Blackbox-Verfahren aufzubewahren. Eskaliert eine Situation, d. h. wird eine Person gewalttätig oder ist absehbar, dass eine Person mit aller Wahrscheinlichkeit gewalttätig wird und das Sicherheitspersonal eingreifen muss, kann in einer zweiten Stufe die Löschung der Voraufnahmen unterbrochen und die dauerhafte Aufnahme der Bodycam aktiviert werden. Ein permanentes anlassloses Pre-Recording ist hingegen auch dann unzulässig, wenn das erhobene Videomaterial innerhalb eines kurzen Intervalls automatisch überschrieben wird.
– Die Aufnahmen sind in einem Blackbox-Verfahren zu speichern. Das bedeutet, dass die Aufnahmen so aufzubewahren sind, dass ein Zugriff von Unbefugten ausgeschlossen ist (Passwortschutz, Verschlüsselung etc.).
– Um die Sicherheit und Integrität der Aufnahmen zu wahren, sind Ort und Datum/Zeit in die Videos einzubetten. Die Videos sind zusammen mit einem Hashwert zu speichern. Damit Aufnahmen nicht manipuliert werden, ist jeder Verarbeitungsschritt zu protokollieren, insbesondere jeder Zugriff. Die aufnehmende Person darf keine Zugriffsberechtigung erhalten.
– Der Fokus der Kamera muss so eingestellt sein, dass ein begrenzter Bildausschnitt aufgenommen und damit möglichst wenig Unbeteiligte betroffen sind.
– Verantwortliche müssen in einem Zugriffs- und Berechtigungskonzept festlegen, wann welcher Personenkreis auf die Aufnahmen zugreifen darf. Eine Auswertung oder ein Zugriff auf die Daten darf nur zu festgelegten

Zwecken erfolgen, etwa um die Aufnahmen an die zuständige Ermittlungsbehörde zu übermitteln oder um eigene zivilrechtliche Ansprüche zu begründen. Nicht benötigte Daten müssen unverzüglich irreversibel gelöscht werden. Eine längere Speicherdauer ist nur dann gerechtfertigt, wenn die Aufnahmen für die Wahrnehmung berechtigter Interessen erforderlich sind wie z. B. die Wahrung zivilrechtlicher Ansprüche.

– Verantwortliche müssen die Datenverarbeitung in das Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO aufnehmen.
– Der Einsatz der Bodycam muss regelmäßig evaluiert werden. Insbesondere ist festzustellen, ob und wie weit der Regeleinsatz dazu führt, dass z. B. Übergriffe auf entsprechend ausgestattetes Personal rückläufig sind.
– Eine Tonaufnahme ist grundsätzlich unzulässig.[2]
– Aufnahmen von Bodycams erlauben Rückschlüsse auf das Verhalten und die Leistung der Beschäftigten. Die Verarbeitung der personenbezogenen Daten ist in einer Betriebsvereinbarung konkret zu beschreiben und festzulegen (vgl. § 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz).

IV.
Transparenz

Die DS-GVO hat die Anforderungen an die Transparenz erhöht. Allein die Bekleidungsaufschrift „Videoüberwachung“ ist nicht ausreichend, um die Informationspflichten zu erfüllen. Nach Art. 13 DS-GVO müssen Betroffenen bereits bei der Erhebung umfangreiche Informationen über die Datenverarbeitung mitgeteilt werden, die weit über den bloßen Umstand der Videoüberwachung hinausgehen.

Sollte es zu Aufnahmen kommen, sind Betroffene unverzüglich in geeigneter Form über die Datenerhebung zu informieren, z. B. durch die Aushändigung eines Merkblattes, welches unter anderem über die Rechtsgrundlage und das berechtigte Interesse hinter dem Bodycam-Einsatz, die Rechte Betroffener, die Speicherdauer, beabsichtigte Übermittlungen sowie über die Kontaktdaten der oder des Verantwortlichen aufklärt.[3]

Auch vor diesem Hintergrund ist der Einsatz einer Pre-Recording-Funktion nicht mit der gegenwärtigen Rechtslage zu vereinbaren. Beim Pre-Recording – gleich welcher Dauer – werden permanent unbeteiligte Passanten

---

2 Ihre unbefugte Anfertigung ist nach §§ 201 Abs. 1, 201a Abs. 1 Strafgesetzbuch, § 33 Kunsturhebergesetz strafbewehrt.

3 Ausführlich: Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, angenommen am 29. November 2017, zuletzt überarbeitet und angenommen am 11. April 2018.

aufgenommen, ohne dass diese über den Umstand der Videoüberwachung gemäß Art. 13 DS-GVO informiert werden können oder dieser ausweichen können. Die Transparenzvorgaben gemäß Art. 5 Abs. 1, 12 ff. DS-GVO sind auch beim Pre-Recording zu beachten. Ist diese Funktion dauerhaft aktiviert, werden permanent unbeteiligte Passanten aufgenommen, ohne dass diese über den Umstand der Videoüberwachung rechtzeitig informiert werden können, um dieser auszuweichen. Auch deshalb darf die Pre-Recording-Funktion nur anlassbezogen aktiviert werden (siehe oben).

3.6
Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung – Stand 29. März 2019

1.
Vorbemerkung

Anbieter von Online-Diensten, die personenbezogene Daten von Nutzerinnen und Nutzern verarbeiten, fallen unter die Regelungen der DS-GVO. Sie haben insbesondere die Vorschriften zur Sicherheit der Verarbeitung (Art. 32) zu beachten. Hierzu gehören auch Maßnahmen zur Sicherung des Zugangs zu den Diensten.

Die vorliegende Orientierungshilfe beschreibt Maßnahmen, die nach Ansicht der Datenschutzaufsichtsbehörden dem Stand der Technik entsprechen und einen effektiven Schutz gewährleisten können. Die Auswahl und Implementation obliegt den Anbietern der Online-Dienste in eigener Verantwortung (Art. 24 DS-GVO).

Anbieter von Online-Diensten sollten sich zudem an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik im IT-Grundschutz-Kompendium zum Identitäts- und Berechtigungsmanagement orientieren (u. a. Basisanforderung ORP.4.A8 „Regelung des Passwortgebrauchs“ oder ORP.4.A11 „Zurücksetzen von Passwörtern“).

2.
Maßnahmen zur Zugangssicherung

2.1
Passwortstärke messen und anzeigen

Die Stärke der von den Nutzerinnen und Nutzern gewählten Passwörter muss gemessen und angezeigt werden, um eine sichere Passwortvergabe zu unterstützen. Hierbei sind insbesondere die Länge, der Einsatz von Ziffern-/Sonderzeichen, Zeichenketten aus Wörterbüchern, landesspezifische Tasta-

turhäufungen (z. B. qwertz), unsichere Trivialpasswörter (z. B. 1234567890) sowie unsichere triviale Ersetzungen von Zeichen (wie o durch 0 oder I durch 1) zu berücksichtigen. In Abhängigkeit der kryptographischen Speicherverfahren sind dabei in der Regel Passwortlängen von mindestens 10 Zeichen erforderlich, um von einem angemessenen Passwort mittlerer Güte zu sprechen. Zudem sollte sichergestellt sein, dass bereits kompromittierte Passwörter nicht erneut genutzt werden dürfen.

2.2
Passwortwechsel nur in Sonderfällen erzwingen

Sofern starke Passwörter (nach 2.1) verwendet werden, ist ein regelmäßiger Passwortwechsel nicht zwingend erforderlich. Der Wechsel von Passwörtern soll insbesondere dann erzwungen werden, wenn der Dienstanbieter ein Initialpasswort in einer Weise zugeteilt hat, dass eine Kenntnisnahme durch Dritte nicht ausgeschlossen werden kann (z. B. durch postalischen Versand), oder wenn Hinweise auf eine Kompromittierung des Kontos oder sicherheitsrelevante Schwachstellen eingesetzter Softwarekomponenten vorliegen.

2.3
Umgang mit fehlgeschlagenen Anmeldeversuchen

Das Fehlschlagen von Anmeldeversuchen ist zu registrieren und der bzw. dem Berechtigten beim nächsten erfolgreichen Login anzuzeigen. Nach einer anwendungsabhängig festzulegenden Anzahl von Fehlversuchen sollte die Anmeldung zeitweise oder dauerhaft gesperrt werden. Dabei sollen sowohl Angriffsversuche auf ein konkretes Konto mit sich ändernden Passwörtern als auch auf viele verschiedene Konten mit sich nicht/kaum ändernden Passwörtern wirksam berücksichtigt werden.

2.4
Umgang mit kompromittierten Diensten

Sollte ein Anbieter Kenntnis erlangt haben, dass sein angebotener Dienst kompromittiert worden ist, so muss er entsprechend Artikel 33 DS-GVO die zuständige Aufsichtsbehörde und seine Nutzer ohne zeitliche Verzögerung darüber informieren. Zudem sind geeignete Maßnahmen zu ergreifen, die dafür sorgen, dass Unbefugte mit diesen kompromittierten Informationen keinen Zugriff auf die Konten erhalten.

2.5
Sinnvolle Benachrichtigungen

Anbieter sollten ihre Nutzer über wichtige Ereignisse informieren, etwa darüber, dass gerade eine Telefonnummer oder eine E-Mail-Adresse geändert wurde, über die der Zugang zu einem Konto ermöglicht wird. Hierzu zählen auch erfolgreiche Logins aus anderen Ländern.

2.6
Sicheres Passwort-Reset

Es sind Passwort-Reset-Verfahren anzubieten, die gegen unbefugte Zugriffsversuche und Social Engineering resistent sind. Verfahren, die ein neues Passwort per E-Mail versenden, sind ungeeignet. Stand der Technik sind Passwort-Reset-Links, bei denen der Link nur ein einziges Mal funktioniert und nur eine kurze Gültigkeitsdauer besitzt (max. eine Stunde). Insbesondere für das Recovery von E-Mail-Konten muss ein zweiter Kanal verwendet werden.

Zusätzliche Sicherheitsfragen beim Anstoßen eines Passwort-Reset-Verfahrens bieten eine größere Sicherheit als ein Versand eines Passwort-Reset-Links ohne weitere Authentisierung, können aber einen zweiten sicheren Kanal nicht ersetzten. Wenn Sicherheitsfragen zum Einsatz kommen, sollten mehrere Fragen eingesetzt werden und neben vorgegebene Fragen auch nutzergenerierte Fragen möglich sein. Fehleingaben bei Sicherheitsfragen müssen wie Fehleingaben von Passwörtern zumindest zu temporären Sperrungen führen.

2.7
Passwörter verschlüsselt übertragen

Passwörter sind vom Nutzer bei der Registrierung und Nutzung über einen nach Stand der Technik kryptographisch abgesicherten Transportkanal an den Endpunkt des Diensteanbieters zu übertragen. Dort muss sichergestellt werden, dass diese in der Server-Anwendung unmittelbar in ein geeignetes Hashverfahren (siehe 2.8) überführt werden.

2.8
Passwörter verschlüsselt speichern

Anbieter dürfen Passwörter nur nach Verarbeitung mittels kryptographischer Einwegverfahren (insbesondere (Salted-)Hashverfahren) nach Stand der Technik speichern. Eine Speicherung mittels symmetrischer Verschlüsselungsalgorithmen (z. B. AES) ist in der Regel nicht notwendig und führt zu

einem erhöhten Risiko, sollte der Verschlüsselungsschlüssel neben den verschlüsselten Daten entwendet werden.

2.9
Passwort-Datenbanken vor unbefugtem Zugriff sichern

Anbieter müssen die Datenbanken, in denen sie Nutzerpasswörter speichern, vor unbefugtem Zugriff durch eigenes Personal und Dritte sichern. Dazu sind regelmäßig unabhängige Penetrations- und Schwachstellentests durchzuführen.

2.10
Schulung der Beschäftigten von Anbietern

Anbieter müssen ihre Beschäftigten regelmäßig zu Fragen des Datenschutzes und der Informationssicherheit schulen. Dies betrifft insbesondere Schulungen, um die Beschäftigten für Social-Engineering-Angriffe zu sensibilisieren.

2.11
Zwei-Faktor-Authentisierung anbieten

Zusätzlich zum Passwortschutz soll eine Zwei-Faktor-Authentisierung angeboten werden. Der zweite Faktor muss auf einem anderen Gerät, einem anderen Kommunikationskanal oder einer anderen ausreichenden Trennung zwischen Passwort und Verwaltung des zweiten Faktors basieren. Einmal aktiviert, darf die Zwei-Faktor-Authentisierung nur unter Verwendung angemessen sicherer Verfahren deaktiviert werden können. Eine Zwei-Faktor-

Authentisierung ist bei Verarbeitungen mit hohem Risiko keine reine Empfehlung, sondern zum Erreichen eines angemessenen Schutzniveaus notwendig. Dabei sollen bevorzugt offene Verfahren wie Time-based One-time Password Algorithmus (TOTP) angeboten werden, die nicht mit einer Offenbarung zusätzlicher personenbezogener Daten (Mobilfunknummern) verbunden sind. Werden durch den Anbieter der Zwei-Faktor-Authentisierung dennoch personenbezogene Daten wie Mobilfunknummern verarbeitet, sind geeignete Garantien anzubieten, welche eine Zweckbindung der Daten ausschließlich für die Zwei-Faktor-Authentisierung dauerhaft sicherstellen. Weiterhin sollten standardisierte Verfahren wie bspw. WebAuthn unterstützt werden.

2.12
Trennung von Authentifikations- und Nutzdaten

Um die Folgen einer möglichen Kompromittierung von Daten zu beschränken, sollen die zur Authentifikation verwendeten Daten, insbesondere Passwörter, logisch getrennt in unterschiedlichen Datenbank-Instanzen von den Inhaltsdaten gespeichert werden. Dies kann auch durch eine gesonderte Verschlüsselung der Inhaltsdaten bewirkt werden.

2.13
Über Passwort-Manager informiere**n**

Nutzerinnen und Nutzern sollen über geeignete Passwort-Manager-Lösungen und deren Gebrauch informiert werden.

2.14
Sicherheit als integrierte Aufgabe

Zur Erreichung eines angemessenen Schutzniveaus muss die Sicherheit einer Anwendung als Ganzes betrachtet werden. Der Umgang mit Passwörtern und der Einsatz eines wirksamen Authentisierungsverfahrens stellen dabei einen wichtigen Baustein dar. Das Sicherheitskonzept einer Anwendung muss gemäß Art. 32 DS-GVO regelmäßig auditiert, evaluiert und verbessert werden. Auch die Grundsätze des Data-Protection-by-Design und Data-Protection-by-Default (Art. 25 DS-GVO) sind zu beachten.

3.7
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – März 2019

Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien

Inhalt

I.
Einführung

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichte am 26. April 2018 eine Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018. Gleichzeitig beschlossen die Datenschutzbehörden, eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen durchzuführen.

Als Ergebnis der Auswertung der Stellungnahmen im Konsultationsverfahren und zur Erläuterung und Konkretisierung der Positionsbestimmung haben die Datenschutzbehörden die folgende Ergänzung formuliert. Das Papier soll gleichzeitig als Orientierungshilfe für die Umsetzung der datenschutzrechtlichen Anforderungen an die Verarbeitung der Daten von Nutzer*innen[4] durch Telemediendienste dienen.

Die Orientierungshilfe steht unter dem ausdrücklichen Vorbehalt eines zukünftigen – möglicherweise abweichenden – Verständnisses der maßgeblichen Vorschriften durch den Europäischen Datenschutzausschuss (EDSA) sowie einer etwaigen Rechtsänderung durch ein zukünftiges Inkrafttreten einer Überarbeitung der Richtlinie 2002/58/EG.

II.
Keine Anwendbarkeit der datenschutzrechtlichen Vorschriften des TMG

Das Telemediengesetz (TMG) ist nach wie vor in all seinen Bestandteilen in Kraft. Eine Anpassung der datenschutzrechtlichen Vorschriften des TMG (4. Abschnitt; §§ 11 ff. TMG) an die Datenschutz-Grundverordnung (DSGVO) wurde nicht vorgenommen. Ein formeller Umsetzungsakt der ePrivacy-Richtlinie 2002/58/EG in der Fassung der Änderung durch die Richtlinie 2009/136/EG[5] (ePrivacy-Richtlinie) ist im 4. Abschnitt des TMG nicht erfolgt.[6] Insbesondere fehlt es an einem Umsetzungsakt für Art. 5 Abs. 3 der ePrivacy-RL

4 Es sollen sich stets alle Menschen angesprochen fühlen. Aus Gründen der einfacheren Lesbarkeit wird im Folgenden jedoch nur eine Form verwendet.

5 Sofern im Folgenden eine Vorschrift der ePrivacy-Richtlinie genannt wird, ist immer die aktuelle in der Fassung der Änderung durch die Richtlinie 2009/136/EG gemeint.

6 So auch BGH, Beschluss vom 5.10.17, Az.: I ZR 7/16, Rz. 16; in Bezug auf Art. 5 Abs. 3 der ePrivacy-Richtlinie 2002/58/EG in der Fassung der Änderung durch die Richtlinie 2009/135/EG vgl. die von der EU-Kommission veröffentlichte Studie: „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (SMART 2013/0071), Final report, 2015, Ziff. 5.2, abrufbar unter: https://ec.europa.eu/digitalsingle-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

im deutschen Recht insgesamt.[7] Es stellt sich daher die Frage nach der Anwendbarkeit der Vorschriften des 4. Abschnitts des TMG seit der Geltungserlangung der DSGVO.

1.
Anwendungsvorrang der DSGVO und Kollisionsregel in Art. 95 DSGVO

Grundsätzlich werden mitgliedstaatliche datenschutzrechtliche Regelungen aufgrund des Anwendungsvorrangs der DSGVO durch diese verdrängt, wenn es keine spezifischen Regelungen gibt, die ein Fortbestehen bereits existierender Regelungen anordnen oder Öffnungsklauseln Spielräume zur mitgliedstaatlichen Ausgestaltung offen lassen beziehungsweise vorgeben. Die DSGVO enthält in Artikel 95 eine Kollisionsregel zum Verhältnis der DSGVO zur ePrivacy-Richtlinie. Danach werden natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union durch die DSGVO keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der ePrivacy-Richtlinie festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Richtlinien bedürfen gemäß Art. 288 AEUV im Unterschied zu Verordnungen der Umsetzung durch die Mitgliedstaaten. Grundsätzlich entfaltet erst das in Umsetzung der Richtlinie geschaffene mitgliedstaatliche Recht Rechtswirkung gegenüber Einzelnen; eine Richtlinie selbst kann keine Verpflichtungen für Einzelne begründen. Die Kollisionsregel in Art. 95 DSGVO umfasst daher die in Umsetzung der ePrivacy-Richtlinie erlassenen mitgliedstaatlichen Vorschriften. Dies betrifft vor allem die Regelungen des Telekommunikationsgesetzes (TKG), die als Umsetzung der ePrivacy-Richtlinie 2002/58/EG anzusehen sind. Durch die Richtlinie 2009/136/EG wurde der Anwendungsbereich der ePrivacy-Richtlinie ausgeweitet. Die Regelung des Art. 5 Abs. 3 ePrivacy-RL adressiert nicht lediglich Anbieter von öffentlichen Telekommunikationsdiensten, sondern auch Anbieter von „Diensten der Informationsgesellschaft". Diese entsprechen den Diensten, die in Deutschland als Telemediendienste bezeichnet und durch das TMG reguliert werden. Spezielle datenschutzrechtliche Vorgaben finden sich in den §§ 11 ff. des TMG. Diese können jedoch nur dann neben der DSGVO zur Anwendung kommen, wenn es sich dabei um Umsetzungen der ePrivacy-Richtlinie handelt und sie somit der Kollisionsregel des Art. 95 DSGVO unterfallen.

7 S. dazu den Final Report, Fn. 3, a. a. O.

2.
Keine Umsetzung der ePrivacy-Richtlinie durch §§ 12, 15 Abs. 1 TMG

Aus den Antworten auf einen Fragebogen der EU-Kommission zur Umsetzung des Art. 5 Abs. 3 ePrivacy-RL geht hervor, dass die Anforderungen des Art. 5 Abs. 3 ePrivacy-RL durch die bereits vorher bestehenden Regelungen in § 12 und § 15 TMG als hinreichende Umsetzung der Richtlinie angesehen worden sind. In den Antworten auf den Fragebogen wird durch die BReg ausgeführt, dass § 12 TMG klarstelle, personenbezogene Daten dürften im Zusammenhang mit der Bereitstellung von Telemedien ohne Einwilligung nur verarbeitet werden, wenn der Gesetzgeber dies ausdrücklich erlaubt. Eine solche gesetzliche Erlaubnis enthalte § 15 TMG. Für die Speicherung und den Abruf von Informationen, wie z. B. Cookies, bedeute dies, dass solche Verfahren in Deutschland ohne Einwilligung der Nutzer nur zulässig seien, wenn dies aus technischen Gründen für die Inanspruchnahme erforderlich sei.

Im Übrigen dürften solche Verfahren ohne Einwilligung des Nutzers nicht verwendet werden.[8] Im Ergebnis bedeute dies, dass der deutsche Gesetzgeber davon ausgegangen ist, dass eine Umsetzung in Form einer gesetzlichen Anpassung nicht erforderlich ist, da sich das Einwilligungserfordernis des Art. 5 Abs. 3 ePrivacy-RL bereits aus § 12 und § 15 Abs. 1 TMG,[9] d. h. aus dem grundsätzlichen Konzept des Verbots mit Erlaubnisvorbehalt ergebe. Mangels gesetzlicher Erlaubnis in § 15 Abs. 1 TMG für die in Art. 5 Abs. 3 ePrivacy-RL geregelten Sachverhalte komme die allgemeine Regel des § 12 TMG, d. h. die Umsetzung des in Art. 7 Buchst. a DSRL geregelten Verbots mit Erlaubnisvorbehalt, zur Anwendung.[10] Auch eine Studie der EU-Kommission[11], die sich mit der Umsetzung der ePrivacy-RL in den einzelnen Mitgliedstaaten befasst, kommt zu dem Ergebnis, dass die Bestimmung vom deutschen Gesetzgeber nicht umgesetzt wurde. Dort heißt es, dass in Deutschland die Auffassung vertreten worden sei, dass die bestehenden Vorschriften des Telemediengesetzes über die Verarbeitung personenbezogener Daten durch (informationsgesellschaftliche) Dienstleister ausreichten, um Nutzer und Teilnehmer zu schützen.[12]

---

8 S. dazu den Final Report, a. a. O.

9 Conrad/Haussen in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 36 Rn. 12.

10 BGH Beschluss vom 5.10.17, Az.: I ZR 7/16, Rz. 22 mit weiteren Nachweisen.

11 EU-Kommission, „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (SMART 2013/0071), Final report, 2015.

12 EU-Kommission, „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regu-lation“ (SMART 2013/0071), Final report,

Die Konstruktion der „Umsetzung“ durch das Verbot mit Erlaubnisvorbehalt in § 12 i. V. m. § 15 Abs. 1 TMG gerät allerdings bereits aufgrund der Entscheidungen des EuGH zu dynamischen IP-Adressen und des Urteils des BGH vom 16. Mai 2017 zur gebotenen richtlinienkonformen Auslegung des § 15 Abs. 1 TMG ins Straucheln. Denn die richtlinienkonforme Auslegung erfordert nach Auffassung des BGH, dass § 15 Abs. 1 TMG dahingehend auszulegen ist, dass „ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung auch über das Ende eines Nutzungsvorgangs hinaus nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit der Dienste zu gewährleisten“. Diese weitergehende Erlaubnis geht über die Möglichkeiten hinaus, die nach den engen Ausnahmeregelungen in Art. 5 Abs. 3 Satz 2 ePrivacy-RL ohne Einwilligung zulässig sind, da die Daten über den Nutzungsvorgang hinaus zur generellen Funktionsfähigkeit gespeichert bleiben können.

Zudem ist zu berücksichtigen, dass die §§ 12 und 15 TMG keine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie, sondern vielmehr eine Umsetzung von Art. 7 Datenschutzrichtlinie 95/46/EG (DSRL) darstellen. Gem. Art. 94 Abs. 1 DSGVO wurde die DSRL mit Wirkung zum 25. Mai 2018 aufgehoben. Die Regelungen zur Rechtmäßigkeit der Verarbeitung personenbezogener Daten werden nunmehr in Art. 6 DSGVO getroffen. Dort findet sich auch die Vorgabe, dass eine Datenverarbeitung nur dann rechtmäßig ist, wenn mindestens eine der in Art. 6 Abs. 1 genannten Voraussetzungen erfüllt ist. Für eine Wiederholung des Verbots mit Erlaubnisvorbehalt im nationalen Recht in Form von § 12 TMG besteht neben der DSGVO damit kein Raum.[13]

Die Kollisions-Regelung des Art. 95 DSGVO bezieht sich außerdem auf „besondere in der Richtlinie 2002/58/EG festgelegte Pflichten“. Solche „besonderen“ Pflichten ergeben sich aus dem allgemeinen Konzept des Verbots mit Erlaubnisvorbehalt gerade nicht.

Im Ergebnis lässt sich festhalten, dass Art. 95 DSGVO für § 12 und § 15 Abs. 1 TMG nicht zur Anwendung kommt.

2015, Ziff. 5.2, abrufbar unter: https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-andcompatibility-proposed-data.

13 S. statt vieler Nettesheim, in: Grabitz/Hilf/ders. (Hrsg.), Das Recht der EU, AEUV, Art. 288, Rn. 101 f., m. w. N.

3.
Keine Umsetzung der ePrivacy-Richtlinie durch § 15 Abs. 3 TMG

Anders als die Bundesregierung nimmt der BGH in seinem Vorlagebeschluss vom 5. Oktober 2017[14] im Hinblick auf die Umsetzung des Art. 5 Abs. 3 ePrivacy-RL vorrangig § 15 Abs. 3 TMG in den Blick.[15] Dies ist folgerichtig vor dem Hintergrund, dass Art. 5 Abs. 3 ePrivacy-RL auch das Speichern oder den Zugriff auf Informationen, die im Endgerät der Nutzer gespeichert sind, erfasst, wie beispielsweise die Verwendung von Cookies. § 15 Abs. 3 TMG stellt eine gesetzliche Erlaubnis für die Erstellung von Nutzungsprofilen unter Pseudonym bereit, womit auch Nutzungsprofile gemeint sein können, die etwa mit Hilfe von Cookies erstellt werden. Im Hinblick auf die Frage der Umsetzung des Art. 5 Abs. 3 ePrivacy-RL ist daher eine Auseinandersetzung mit § 15 Abs. 3 TMG und die Prüfung einer richtlinienkonformen Auslegung geboten.

Gemäß § 15 Abs. 3 TMG durfte der Diensteanbieter zu Zwecken der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung eines Pseudonyms erstellen, sofern die Nutzer nicht widersprechen. Die in § 15 Abs. 3 TMG genannten Zwecke entsprechen nicht den Ausnahmetatbeständen des Art. 5 Abs. 3 Satz 2 der ePrivacy-RL. Das bedeutet, dass für die in § 15 Abs. 3 TMG genannten Zwecke nach Art. 5 Abs. 3 ePrivacy-RL grundsätzlich eine Einwilligung der Teilnehmer oder Nutzer erforderlich ist. Die Einwilligung i. S. der ePrivacy-Richtlinie ist gemäß deren Art. 2 Satz 2 lit. f) eine Einwilligung i. S. d. DSRL. Gemäß Art. 94 Abs. 2 DSGVO werden Verweise auf die DSRL zu Verweisen auf die DSGVO, so dass die Frage, welche Anforderungen an eine Einwilligung zu stellen sind, ab dem 25. Mai 2018 nach Maßgabe der DSGVO zu beantworten ist. Hieran ändert auch Art. 95 DSGVO nichts. Die Einwilligung ist in der ePrivacy-Richtlinie, wie erwähnt, nicht eigenständig geregelt, so dass insofern keine lexspecialis-Situation besteht.[16]

Hinweis:

Der maßgebliche Unterschied zwischen einer Widerspruchslösung (Opt-Out) und einer Einwilligung (Opt-In) ist, dass im Falle einer Widerspruchslösung zunächst eine Datenverarbeitung stattfindet, die lediglich durch Erklärung eines Widerspruchs für die Zukunft untersagt werden kann. Anders liegt der Fall hingegen, wenn eine Einwilligung (Opt-In) erforderlich ist. Dann darf

14 BGH, Beschl. v. 5.10.17, I ZR 7/16.

15 BGH, Beschl. v. 5.10.17, I ZR 7/16, Rz. 13, 16.

16 Kühling/Buchner, DSGVO 2017, Art. 95 Rn. 7.

eine Datenverarbeitung nämlich erst stattfinden, nachdem eine wirksame Einwilligung vom Nutzer tatsächlich erteilt worden ist.

Gem. Art. 4 Nr. 11 DSGVO muss die Einwilligung in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung abgegeben werden. Erwägungsgrund 32 ist zu entnehmen, dass „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person […] daher keine Einwilligung darstellen [sollten]". Darüber hinaus ist das Widerspruchsrecht in Abgrenzung zu der Einwilligung gesondert in der DSGVO in Art. 21 geregelt. Vor diesem Hintergrund kann ausgeschlossen werden, dass das Unterbleiben eines Widerspruchs eine Einwilligung i. S. d. DSGVO darstellen kann.

Eine direkte Anwendung des § 15 Abs. 3 TMG als Umsetzung des Art. 5 Abs. 3 ePrivacy-RL in der Fassung der Änderung durch die Richtlinie 2009/136/EG scheidet damit jedenfalls seit dem 25. Mai 2018 aus.

4.
Keine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG

In Betracht kommt für die Beibehaltung nur eine richtlinienkonforme Auslegung des § 15 Abs. 3 TMG, um die Vorschrift über Art. 95 DSGVO weiterhin anzuwenden. Dazu stellt sich zunächst die Frage, ob § 15 Abs. 3 TMG, d. h. die Widerspruchslösung, so angewendet werden kann, dass dies nicht zu einem der Richtlinie widersprechenden Ergebnis führt. Dies ist jedenfalls seit dem 25. Mai 2018 nicht der Fall. Die Widerspruchslösung erfüllt nicht die Anforderungen an eine Einwilligung gemäß Art. 7 DSGVO.

5.
Keine Öffnungsklausel für nicht-öffentliche Stellen

Die Beibehaltung der Regelungen der §§ 12, 15 Abs. 1 und 15 Abs. 3 TMG kann für nicht-öffentliche Stellen auch nicht durch eine Öffnungsklausel der DSGVO gerechtfertigt werden. Damit sind die Regelungen im nationalen Recht, die nach Ansicht des deutschen Gesetzgebers eine Umsetzung von Art. 5 Abs. 3 ePrivacy-RL darstellen oder für eine solche Umsetzung in Betracht kommen, nicht mehr anwendbar.

6.
Keine unmittelbare Anwendung

Auch eine unmittelbare Anwendung der ePrivacy-Richtlinie kommt nicht in Betracht. Nach der Rechtsprechung des EuGH können sich Einzelne zwar unter bestimmten Voraussetzungen gegenüber einem umsetzungssäumigen

Mitgliedstaat unmittelbar auf eine Bestimmung einer EU-Richtlinie berufen.[17] Voraussetzungen sind u. a. eine fehlende oder mangelhafte Umsetzung[18] sowie, dass die Norm der Richtlinie inhaltlich unbedingt und hinreichend genau ist.[19] Eine Richtlinie kann jedoch nicht selbst Verpflichtungen für Private begründen.[20]

7.
Zwischenergebnis

Da Art. 5 Abs. 3 ePrivacy-Richtlinie in Deutschland nicht umgesetzt wurde und weder eine richtlinienkonforme Auslegung noch eine unmittelbare Wirkung des Art. 5 Abs. 3 ePrivacy-Richtlinie in Betracht kommt, entstehen hieraus für Telemediendiensteanbieter in Deutschland keine bereichsspezifischen Pflichten im Sinne des Art. 95 DSGVO, so dass dessen Voraussetzungen insoweit nicht greifen. Zudem finden sich auch keine Öffnungsklauseln in der DSGVO, die die Anwendbarkeit des § 15 TMG rechtfertigen. Es bleibt daher bei der generellen Anwendung der Regelungen der DSGVO.

III.
Rechtmäßigkeit der Verarbeitung

1.
Einführung

Zur Vereinfachung bei der Bezugnahme auf bestimmte Vorgänge im Bereich der Nutzungsdatenverarbeitung verwendet die Positionsbestimmung u. a. den Begriff „Tracking“. Nach dem Verständnis der Aufsichtsbehörden handelt es sich bei „Tracking“ um Datenverarbeitungen zur – in der Regel website-übergreifenden – Nachverfolgung des individuellen Verhaltens von Nutzern.

---

17 BVerfGE 75, 223; EuGH, Slg. 2002, I-6325, (Marks & Spencer), Rn. 24.

18 EuGH, Rs. 152/84, Slg. 1986, 723, (Marshall I), Rn. 46.

19 EuGH, Rs. 148/78, Slg. 1979, 1629, (Ratti), Rn. 23. 17 EuGH, Rs. 152/84, Slg. 1986, 723, (Marshall I), Rn. 48; Verb. Rs. 372 bis 374/85, Slg. 1987, 2141, (Traen), Rn. 24; Rs. 14/86, Slg. 1987, 2545, (Pretore di Salò/X), Rn. 19; Rs. 80/86, Slg. 1987, 3969, (Kolpinghuis Nijmegen), Rn. 9; Rs. C221/88, Slg. 1990, I-495, (Busseni), Rn. 23; Rs. C-106/89, Slg. 1990, I-4135 (Marleasing), Rn. 6; Rs. C-168/95, Slg. 1996, I-4705 (Arcaro), Rn. 36 ff.; Rs. C-97/96, Slg. 1997, I-6843 (Daihatsu Deutschland), Rn. 24; Rs. C-201/02, Slg. 2004, I-723 (Delena Wells), Rn. 56.

20 EDPB, Leitlinie zur Einwilligung, WP 259, S. 16. 21. Vgl. dazu auch Aufforderungsschreiben der CNIL an Vectaury vom 9. November 2018, Informationen dazu abrufbar unter https://www.cnil.fr/en/node/24929.

Dieses Begriffsverständnis entspricht dem, welches von den europäischen Aufsichtsbehörden in Veröffentlichungen zugrunde gelegt wird.[21]

Für die Bewertung der Zulässigkeit ist aber allein entscheidend, ob eine bestimmte Verarbeitungstätigkeit rechtmäßig durchgeführt wird und der Verantwortliche allen datenschutzrechtlichen Pflichten der DSGVO nachkommt. Die Datenverarbeitung ist nur dann rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 DSGVO vorliegt.

2.
Rechtmäßigkeit der Verarbeitung

Sämtliche Erlaubnistatbestände der DSGVO sind als gleichrangig und gleichwertig zu betrachten. In Art. 6 DSGVO werden die Bedingungen für die rechtmäßige Verarbeitung personenbezogener Daten festgelegt und sechs Rechtsgrundlagen beschrieben, auf die sich Verantwortliche stützen können.[22] Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche bei der Erbringung von Telemediendiensten kommen insbesondere folgende Erlaubnistatbestände in Betracht:

a. Art. 6 Abs. 1 lit. a) DSGVO – Einwilligung
b. Art. 6 Abs. 1 lit. b) DSGVO – Vertrag
c. Art. 6 Abs. 1 lit. f) DSGVO – Interessenabwägung

Hinweis:

Verantwortliche müssen im Rahmen ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachweisen, dass die Verarbeitung personenbezogener Daten rechtmäßig erfolgt. Dies bedeutet, dass Verantwortliche vorab prüfen und dokumentieren müssen, auf welchen

Erlaubnistatbestand sie die Verarbeitung stützen. Die Nutzer müssen über die Erlaubnistatbestände für sämtliche Verarbeitungen ihrer personenbezogenen Daten informiert werden (Informationspflichten nach Art. 13 f. DSGVO).

Im Folgenden werden die o. g. Erlaubnistatbestände näher erläutert.

---

21 Art. 29 Datenschutzgruppe, WP 194 vom 7. Juni 2012, S. 10; EDPB, Leitlinie zur Einwilligung, WP 259, S. 4 (abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp259-rev-0_1_DE.PDF).

22 EDPB Leitlinie zur Einwilligung, WP 259, S. 27 (abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp259-rev-0_1_DE.PDF).

a) Art. 6 Abs. 1 lit. a) DSGVO – Einwilligung

Art. 4 Nr. 11 und Art. 7 DSGVO fordern eine selbstbestimmte und informierte Einwilligung der betroffenen Personen in die jeweilige Datenverarbeitung. Dies setzt voraus, dass jegliche Datenverarbeitungen transparent und nachvollziehbar sein müssen. Insbesondere wenn bei

der betroffenen Person erhobene Daten von dem jeweiligen Diensteanbieter (inkl. eingebundener Dienste) website-übergreifend zusammengeführt und ausgewertet werden, ist zu berücksichtigen, dass die betroffenen Personen für eine wirksame Einwilligung vorab über jegliche Form der durchgeführten Datenverarbeitung sowie sämtliche Empfänger ausführlich informiert werden und die Möglichkeit erhalten müssen, in die einzelnen Formen der Datenverarbeitung spezifisch einzuwilligen. In Fällen, in denen sich mehrere (gemeinsame) Verantwortliche auf die ersuchte Einwilligung stützen wollen oder in denen die Daten an andere Verantwortliche übermittelt oder von anderen Verantwortlichen verarbeitet werden sollen, müssen diese Organisationen sämtlich genannt[23] und die Verarbeitungsaktivitäten der einzelnen Organisationen hinreichend beschrieben werden. In diesen Fällen müssen alle beteiligten Akteure überprüfen, ob eine wirksame Einwilligung für ihre Aktivitäten vorliegt und ob diese von ihnen nachgewiesen werden kann (Art. 5 Abs. 2 DSGVO).[21] Eine Verarbeitung personenbezogener Daten ohne ausreichende Kenntnis der betroffenen Personen

– über die jeweiligen Datenverarbeitungsvorgänge,
– über die jeweils einbezogenen Dritten sowie
– ohne Möglichkeit der gesonderten Zustimmung

führt zur Unwirksamkeit der Einwilligung und erfolgt daher ohne Rechtsgrund. Es ist von grundlegender Bedeutung, den betroffenen Personen Informationen bereitzustellen, um von ihnen eine wirksame Einwilligung einholen zu können. Nur so ist es betroffenen Personen möglich, Entscheidungen in Kenntnis der konkreten Sachlage zu treffen und die Reichweite der Einwilligung zu verstehen.

Art. 4 Nr. 11 DSGVO setzt für eine wirksame Einwilligung weiter eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung“ oder eine sonstige eindeutige bestätigende Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten ausdrücklich einverstanden ist. Dies kann beispielweise durch Anklicken eines Kästchens beim Besuch

23 EDPB, Leitlinie zur Einwilligung, WP 259, S. 16. 21. Vgl. dazu auch Aufforderungsschreiben der CNIL an Vectaury vom 9. November 2018, Informationen dazu abrufbar unter https://www.cnil.fr/en/node/24929.

einer Website, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder aktive Verhaltensweise geschehen, mit der die betroffene Person eindeutig ihr Einverständnis hinsichtlich der angekündigten und beabsichtigten Datenverarbeitung ausdrückt.

Opt-Out-Verfahren reichen dafür nicht aus. Insoweit führt Erwägungsgrund 32 DSGVO explizit aus, dass konkludente Verhaltensweisen wie „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person" keine Einwilligungen darstellen.

Hinweis: „Cookie-Banner" & „Consent-Tools"

Durch eine vorgeschaltete Abfrage beim ersten Aufruf einer Website oder einer Web-App kann u. a. eine wirksame Einwilligung für einwilligungsbedürftige[24] Datenverarbeitungen eingeholt werden. Dabei sind jedoch folgende Anforderungen zu beachten:

– Beim erstmaligen Öffnen einer Website erscheint das Banner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses HTML-Element aus einer Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, die unter Nennung der beteiligten Akteure und deren Funktion ausreichend erklärt werden und über ein Auswahlmenü aktiviert werden können. Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht „aktiviert" voreingestellt sein dürfen.
– Während das Banner angezeigt wird, werden zunächst alle weitergehenden Skripte einer Website oder einer Web-App, die potenziell Nutzerdaten erfassen, blockiert. Der Zugriff auf Impressum und Datenschutzerklärung darf durch „Cookie-Banner" nicht verhindert werden.
– Erst wenn der Nutzer seine Einwilligung(en) durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Banner oder den Klick auf eine Schaltfläche abgegeben hat, darf die einwilligungsbedürftige Datenverarbeitung tatsächlich (durch technische Maßnahmen sichergestellt) stattfinden.
– Zur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DSGVO ist es gem. Art. 11 Abs. 1 DSGVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. Erwägungsgrund 26) ist ausreichend. Damit die Entscheidung des Nutzers für oder gegen eine Einwilligung bei einem weiteren Aufruf der Website berücksichtigt wird und das Banner nicht erneut erscheint, kann deren Ergebnis auf

24 Die Nutzung von Cookies ist nicht per se einwilligungsbedürftig. Entsprechende Banner sollen daher nur eingesetzt werden, wenn tatsächlich eine Einwilligung notwendig ist.

dem Endgerät des Nutzers ohne Verwendung einer User-ID o. ä. vom Verantwortlichen gespeichert werden. Durch ein solches Verfahren kann der Nachweis einer vorliegenden Einwilligung erbracht werden.

– Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zum Widerruf implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 S. 4 DSGVO.

Verantwortliche müssen sicherstellen, dass die Einwilligung nicht nur das Setzen von einwilligungsbedürftigen Cookies umfasst, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z. B. Verfahren zur Verfolgung der Nutzer durch Zählpixel oder div. Fingerprinting-Methoden, wenn diese nicht aufgrund einer anderen Rechtsgrundlage zulässig sind.

Auch genügt es für eine Einwilligung i. S. d. DSGVO nicht, wenn, wie bei vielen einfachen Cookie-Bannern im Web, ein Hinweis auf das Setzen von Cookies zusammen mit einem „OK"-Button erfolgt. In diesen Fällen fehlt es an der nach Art. 7 DSGVO erforderlichen Freiwilligkeit, wenn die betroffenen Personen zwar „OK" drücken können, aber keine Möglichkeit erhalten, das Setzen von Cookies abzulehnen.

Die Einwilligung muss freiwillig sein, das heißt ohne Zwang abgegeben werden. Freiwillig ist die Einwilligung nur, wenn die betroffene Person eine echte und freie Wahl hat und somit in die Lage versetzt wird, eine Einwilligung auch verweigern zu können, ohne dadurch Nachteile zu erleiden (Erwägungsgrund 42 DSGVO). Auch eine Koppelung der Erbringung einer vertraglichen Dienstleistung an die Abgabe einer datenschutzrechtlichen Einwilligung führt gem. Art. 7 Abs. 4 DSGVO regelmäßig dazu, dass die Einwilligung nicht als freiwillig angesehen werden kann und damit unwirksam ist.[25] Der Besuch einer Website sollte auch dann noch möglich sein, wenn betroffene Personen sich gegen das Setzen von Cookies entscheiden und nicht in die personenbezogene Datenverarbeitung einwilligen. Eine Einwilligung gilt nach Erwägungsgrund 43 DSGVO auch dann nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann. Wenn bei Websites durch vorgeschaltete Abfragen eine Einwilligung eingeholt wird, müssen die einzelnen Verarbeitungsvorgänge daher gesondert anwählbar sein.

Schließlich ist Art. 25 Abs. 2 DSGVO zu beachten, der von dem datenschutzrechtlich Verantwortlichen verlangt, geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass durch datenschutzfreundliche Voreinstellungen nur personenbezogene Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich

25 EDPB, Leitlinien zur Einwilligung, WP 259, S. 9.

sind. Konsequenterweise sollte nicht zuletzt nach den Grundsätzen „data protection by design“ und „data protection by default“ (Erwägungsgrund 78 DSGVO) sichergestellt werden, dass die technischen Vorrichtungen ebenso datenschutzfreundlich eingestellt sind und damit die Einholung einer wirksamen Einwilligung ermöglichen. Außerdem ist durch den datenschutzrechtlich Verantwortlichen technisch sicherzustellen, dass Verfahren zur Verfolgung von Nutzeraktivitäten, die datenschutzrechtlich einer Einwilligung bedürfen, erst dann zum Einsatz kommen, wenn die betroffene Person die Information über die geplante Datenverarbeitung inhaltlich erfasst und eine Entscheidung in Form einer expliziten Willensbetätigung darüber getroffen hat.

b) Art. 6 Abs. 1 lit. b) DSGVO – Vertrag

Die Verarbeitung personenbezogener Daten des Vertragspartners auf vertraglicher Grundlage ist gemäß Art. 6 Abs. 1 lit. b) DSGVO nur möglich, wenn die Datenverarbeitung zur Erfüllung eines Vertrages oder im Rahmen vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Im Hinblick auf andauernde Diskussionen auf europäischer Ebene zur Frage der Anwendbarkeit des Art. 6 Abs. 1 lit. b) DSGVO im Zusammenhang mit der Bereitstellung von Online-Services wird zum gegenwärtigen Zeitpunkt auf Ausführungen zu Art. 6 Abs. 1 lit. b) DSGVO verzichtet.

c) Art. 6 Abs. 1 lit. f) DSGVO – Interessenabwägung

Bei der Interessenabwägung gem. Art. 6 Abs. 1 lit. f) DSGVO handelt es sich um eine Vorschrift mit einem weiten und unspezifischen Anwendungsbereich. Dies hat einerseits den Vorteil, dass die Vorschrift flexibel ist und auf eine Vielzahl von Sachverhalten angewendet werden kann. Anderseits führt dies zu Rechtsunsicherheiten und Fragen bei der Anwendung im konkreten Einzelfall.

Im Folgenden werden Kriterien aufgestellt, die die Anwendung erleichtern sollen und zugleich helfen können, die Rechenschaftspflichten nach der DSGVO zu erfüllen.

Bei der Verarbeitung personenbezogener Daten auf der Grundlage des Art. 6 Abs. 1 lit. f) DSGVO ist zu berücksichtigen, dass die Vorschrift keinen Auffangtatbestand darstellt. Die Verarbeitung ist nur rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Ob die Voraussetzun-

gen des Art. 6 Abs. 1 lit. f) DSGVO erfüllt sind, ist anhand einer dreistufigen Prüfung zu ermitteln:

1. Stufe: Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten
2. Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung dieser Interessen
3. Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall

Hinweis:

Dieser Prüfungsaufbau soll die Überprüfung der Anforderungen des Art. 6 Abs. 1 lit. f) DSGVO erleichtern und orientiert sich sowohl an der Rechtsprechung des EuGH als auch an der Auffassung der europäischen Aufsichtsbehörden.

1. Stufe:
Vorliegen eines berechtigten Interesses der Verantwortlichen oder eines Dritten

Anbieter von Telemediendiensten können eine Vielzahl von berechtigten Interessen haben.[26] Die DSGVO definiert den Begriff des „berechtigten Interesses" nicht und nennt nur vereinzelt Beispiele für ein berechtigtes Interesse. Das berechtigte Interesse hat eine enge Verbindung zum Verarbeitungszweck und kann wirtschaftlicher, ideeller oder rechtlicher Natur sein. Der Begriff des „berechtigten Interesses" kann als das wesentliche Motiv für die Verarbeitung verstanden werden und spiegelt den Nutzen wider, den der Verantwortliche aus der Verarbeitung ziehen möchte.

Dazu zählt beispielsweise die Erbringung des Dienstes in einer Form, die eine nutzerfreundliche Wahrnehmung des Online-Angebots möglich macht. Ausdrücklich benennt die DSGVO im Erwägungsgrund 47 zudem die Verhinderung von Betrug und die Direktwerbung als mögliche berechtigte Interessen.

Berechtigt meint, dass das Interesse im Einklang mit der Rechtsordnung steht. Das bedeutet, dass jedenfalls illegale oder diskriminierende Beweggründe in keinem Fall ein berechtigtes Interesse begründen können.

Weitere Interessen, die von Telemediendiensteanbietern für die Verarbeitung von Nutzungsdaten genannt werden, sind u. a.:

26 S. im Einzelnen beispielhaft WP 217.

– Bereitstellung besonderer Funktionalitäten, z. B. die Warenkorb-Funktion unter Verwendung eines sog. Session-Identifiers
– Freie Gestaltung der Website auch unter Effizienz- und Kosteneinsparungserwägungen, z. B. Einbindung von Inhalten, die auf anderen Servern gehostet werden, Nutzung von Content Delivery Networks (CDN), Web Fonts, Kartendiensten, Social-Plugins etc.
– Integrität und Sicherheit der Website (IT-Security-Maßnahmen sind bspw. das Speichern von LogDateien und insbesondere IP-Adressen für einen längeren Zeitraum, um Missbrauch erkennen und abwehren zu können)
– Reichweitenmessung und statistische Analysen
– Optimierung des jeweiligen Webangebots und Personalisierung/Individualisierung des Angebots abgestimmt auf die jeweiligen Nutzer
– Wiedererkennung und Merkmalszuordnung der Nutzer, z. B. bei werbefinanzierten Angeboten
– Betrugsprävention, Abwehr von den Dienst überlastenden Anfragen (Denial of Service-Attacken) und Bot-Nutzung

Hinweis:

Die genannten Beispiele können auf der ersten Stufe ein berechtigtes Interesse begründen. Für die Zulässigkeit von Datenverarbeitungen zu diesen Zwecken kommt es aber auf die Erforderlichkeit und die Interessenabwägung an.

2. Stufe:
Erforderlichkeit der Datenverarbeitung zur Wahrung der berechtigten Interessen

Allein das Vorliegen eines berechtigten Interesses reicht nicht aus, um die Datenverarbeitung zu legitimieren. Zwingend ist, dass die jeweilige Datenverarbeitung zur Wahrung dieses Interesses erforderlich ist. Erforderlichkeit meint, dass die Verarbeitung geeignet ist, das Interesse (Motiv/Nutzen der Verarbeitung) des Verantwortlichen zu erreichen, wobei kein milderes, gleich effektives Mittel zur Verfügung steht. Das bedeutet, dass der Verantwortliche die Verarbeitung auf das notwendige Maß zu beschränken hat.

Beispiel:

Der Verantwortliche betreibt eine Website und möchte wissen, wie sein Online-Angebot angenommen wird und ob gegebenenfalls Verbesserungen erforderlich sind. Dazu möchte er wissen, wie viele Nutzer die Website in einem bestimmten Zeitraum besuchen, welche Geräte die Nutzer verwenden

und welche Spracheinstellungen sie haben. Der Verantwortliche benötigt diese Informationen, um sein Webangebot zu optimieren und die Darstellung an die Endgeräte anzupassen.

Die Messung der Reichweite und die sich daraus ergebenden Informationen sind geeignet, um das Webangebot anzupassen (berechtigtes Interesse). Setzt der Website-Betreiber hierfür ein Analyse-Tool ein, welches Daten über das Nutzungsverhalten betroffener Personen an Dritte weitergibt (z. B. soziale Netzwerke oder externe Analysedienste, die Nutzungsdaten über die Grenze der Website hinweg mit Daten von anderen Websites zusammenführen), ist dies nicht mehr erforderlich. Das Ziel – Reichweitenmessung – kann auch mit milderen, gleich geeigneten Mitteln erreicht werden, die deutlich weniger personenbezogene Daten erheben und diese nicht an Dritte übermitteln (z. B. ohne Einbindung Dritter über eine lokale Implementierung einer Analysesoftware).

3. Stufe:
Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall

Dem berechtigen Interesse des Verantwortlichen stehen die Interessen sowie Grundrechte und Grundfreiheiten der Nutzer gegenüber.

Darunter fällt nicht nur das Recht auf Schutz personenbezogener Daten gem. Art. 8 Charta der Grundrechte der Europäischen Union (GRCh) oder das Recht auf Vertraulichkeit der Kommunikation gem. Art. 7 GRCh, sondern auch die Freiheit der Meinungsäußerung sowie das Interesse an einer freien Informationsgewinnung, Art. 11 GRCh. Auch andere Freiheiten und Interessen der betroffenen Personen sind zu berücksichtigen, beispielsweise das Interesse, keine wirtschaftlichen Nachteile zu erleiden (z. B. bei personalisierter Preisbildung).

Das Recht auf Vertraulichkeit der Kommunikation schützt vor der Verwendung von eindeutigen Identifiern, wie z. B. IMEI-Nummer, IMSI-Nummer, MAC-Adresse oder auch Ad-IDs (gerätespezifische Werbe-Nummern). Daneben geschützt ist auch die (Geräte-)Integrität. Werden z. B. Identifier auf dem Endgerät des Nutzers abgelegt, so ist die Integrität des Gerätes berührt.

Im Rahmen der Abwägung sind die Ausgestaltung der Verarbeitung personenbezogener Daten sowie die konkreten Auswirkungen der Verarbeitung auf die betroffenen Personen zu berücksichtigen. Bei diesem Prüfungsschritt handelt es sich um den **Kern der Interessenabwägung**.

Die ermittelten, sich gegenüberstehenden Interessen sind zu gewichten. Hierfür kann keine allgemeingültige Regel aufgestellt werden. Verantwortliche können sich jedoch an folgenden Grundsätzen orientieren:

– Ein spezifisch, verfassungsrechtlich anerkanntes Interesse, z. B. Recht auf Schutz personenbezogener Daten gem. Art. 8 GRCh, hat ein höheres Gewicht, als ein Interesse, dass nur einfachgesetzlich in der Rechtsordnung anerkannt ist.[27]
– Ein Interesse ist gewichtiger, wenn es nicht nur dem Verantwortlichen dient, sondern gleichzeitig auch der Allgemeinheit, z. B. bei Forschungstätigkeiten, deren Erkenntnisse für medizinische Vorsorge genutzt werden sollen.

Zu beachten ist, dass im Rahmen der Abwägung ohnehin bestehende Pflichten aus der DSGVO, z. B. Informationspflichten oder die Sicherheit der Verarbeitung durch Pseudonymisierung, nicht zugunsten des Verantwortlichen berücksichtigt werden können. Die allgemeinen Pflichten der DSGVO stellen keine „best practices“ dar, sondern sind gesetzliche Anforderungen, die in jedem Fall zu erfüllen sind. Gleichwohl können durch zusätzliche Schutzmaßmaßnahmen die Beeinträchtigungen durch die Verarbeitung derart reduziert werden, dass die Interessenabwägung zugunsten des Verantwortlichen ausfallen kann.

Hinweis:

Im Hinblick auf die Verwendung von Pseudonymen ist generell anzumerken, dass die Tatsache, dass die Nutzer etwa über IDs oder Kennungen bestimmbar gemacht werden, keine Pseudonymisierungsmaßnahme i. S. d. DSGVO darstellt. Zudem handelt es sich nicht um geeignete Garantien zur Einhaltung der Datenschutzgrundsätze oder zur Absicherung der Rechte betroffener Personen, wenn zur (Wieder-)Erkennung der Nutzer IP-Adressen, Cookie-IDs, Werbe-IDs, Unique-User-IDs oder andere Identifikatoren zum Einsatz kommen. Denn, anders als in Fällen, in denen Daten pseudonymisiert werden, um die identifizierenden Daten zu verschleiern oder zu löschen, so dass die betroffenen Personen nicht mehr adressiert werden können, werden IDs oder Kennungen dazu genutzt, die einzelnen Individuen unterscheidbar und adressierbar zu machen. Eine Schutzwirkung stellt sich folglich nicht ein. Es handelt sich daher nicht um Pseudonymisierungen i. S. d. ErwGr 28, die die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Darüber hinaus ist zu berücksichtigen, dass sich Nutzer in den allermeisten Fällen früher oder später an irgendeiner Stelle im Web re-

27 Art. 29-Datenschutzgruppe, WP 217.

gistrieren und in diesen Fällen auch eine Verknüpfung mit E-Mail-Adressen, Klarnamen oder Offline-Adressen möglich ist. Auf die Kenntnis des bürgerlichen Namens zur Identifikation von betroffenen Personen kommt es aber beim Personenbezug nicht an. Wenn die Nutzung des Webs, wie bei vielen Menschen, einen großen Teil der Lebenswirklichkeit widerspiegelt, dann ist es relevant, ob die Nutzer über ihre Online-Kennungen bestimmbar oder adressierbar sind. Die DSGVO geht davon aus, dass eine indirekte Identifizierung auch durch Aussondern erfolgen kann (ErwGr 26 S.3).

Um Art. 6 Abs. 1 lit. f) DSGVO im Einzelfall anzuwenden, können u. a. die Erwägungsgründe der DSGVO unterstützend herangezogen werden. Aus ihnen ergeben sich insbesondere die folgenden Kriterien, die im Einzelfall im Rahmen der Interessenabwägung heranzuziehen sind:

a. Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz
b. Interventionsmöglichkeiten der betroffenen Personen
c. Verkettung von Daten
d. Beteiligte Akteure
e. Dauer der Beobachtung
f. Datenkategorien
g. Umfang der Datenverarbeitung
h. Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen)

a) Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz

Gemäß Erwägungsgrund 47 müssen die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, berücksichtigt werden. Neben den subjektiven Erwartungen der betroffenen Person ist auch zu fragen, was objektiv vernünftigerweise erwartet werden kann. Die Erwartungen können nicht durch die nach der DSGVO vorgesehenen Pflichtinformationen (Art. 13, 14 DSGVO) erweitert werden. Kritisch ist es zu bewerten, wenn verschiedene Akteure zusammenwirken und die datenschutzrechtlichen Beziehungen der Akteure untereinander unklar oder nicht definiert sind (Verantwortlicher, Auftragsverarbeiter, gemeinsame Verantwortliche).

Im Hinblick auf die Einbindung von Diensten Dritter erwartet ein Nutzer üblicherweise nicht, dass an diese Dritten, zu denen der Nutzer regelmäßig keine Beziehungen unterhält, Informationen darüber weitergegeben werden, welche Websites er besucht oder welche Apps er nutzt. Jedenfalls dann,

wenn die Dritten die Nutzerdaten zu eigenen Zwecken weiterverarbeiten, sind die Folgen und potenziellen Risiken für die Interessen, Grundfreiheiten und Grundrechte der betroffenen Personen weder einschätz- noch bewertbar. Dies betrifft insbesondere das Risiko beim Besuch anderer Dienste oder der Nutzung anderer Geräte (wieder-)erkannt zu werden und dadurch z. B. bei der Informationsgewinnung fremdgesteuert zu werden.

Diese Verarbeitungen entsprechen nicht den vernünftigen Erwartungen der Nutzer, weil sie sich im Hinblick auf die Selbstbestimmung nur nachteilig auswirken. Ebenso liegen Techniken, welche das Verhalten von Besuchern bei der Interaktion mit einem Dienst der Informationsgesellschaft exakt nachvollziehen und dokumentieren können, wie z. B. bei der Erfassung der Tastatur-, Maus- und Wischbewegungen auf Touchscreens, außerhalb der Erwartungshaltung des Nutzers.

Beispiel – Reichweitenmessung:

Der Nutzer ruft eine Website auf. Er geht davon aus, dass die Website von einem einzelnen Verantwortlichen zur Verfügung gestellt wird, nämlich von dem, mit dem zum Zeitpunkt eines Aufrufs ein direktes Nutzungsverhältnis besteht.

Dienste von Drittanbietern in Apps oder auf Websites werden von betroffenen Personen jedoch nicht bewusst wahrgenommen und regelmäßig ohne Zutun aktiviert, da der Verantwortliche sie in sein Online-Angebot eingebunden hat (z. B. Zählpixel eines Werbenetzwerks).

Im Gegensatz dazu ist es für den Nutzer vorhersehbar, dass der Verantwortliche die Reichweite seines Online-Angebots misst, etwa um das Online-Angebot bedarfsgerecht zu gestalten. Für diesen Zweck sind keine andauernde Wiedererkennung und stetig umfangreichere Profilbildung sowie keine Weitergabe von Daten an Dritte nötig. Statistische Angaben geben hinreichend Aufschluss über das allgemeine Nutzungsverhalten, so dass die Vorhaltung von individuellen Nutzungsprofilen für den Zweck Reichweitenmessung nicht erforderlich ist. Die Beeinträchtigung des Nutzers ist dann als gering zu bewerten mit der Folge, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt.

b) Interventionsmöglichkeiten der betroffenen Personen

Im Rahmen der Interessenabwägung kann – ggf. auch als Kompensationsmaßnahme – Berücksichtigung finden, in welcher Form die betroffenen Personen Möglichkeiten haben und darüber informiert werden, die personenbezogene

Datenverarbeitung rechtlich wie technisch zu unterbinden, einzuschränken oder unter andere Bedingungen zu setzen.

Dabei kann z. B. die Form des Identifiers, mit dem Geräte oder Nutzer ausgesondert und wiedererkannt werden, eine Rolle spielen. Abhängig vom Identifier kann es für die betroffenen Personen unterschiedliche Möglichkeiten geben, eine Wiedererkennung oder Nachverfolgung des Nutzungsverhaltens einzuschränken. Nutzer können etwa in den Browser-Einstellungen bestimmte Cookies löschen. Beim Device-Fingerprinting hingegen ist es praktisch unmöglich, eine (Wieder-)Erkennung nutzerseitig zu verhindern.

Darüber hinaus können den betroffenen Personen über Art. 21 DSGVO hinausgehende – überobligatorische – Widerspruchsrechte eingeräumt werden. Zwar sieht Art. 21 DSGVO vor, dass die betroffene Person das Recht hat, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die gem. Art. 6 Abs. 1 lit. f) erfolgt, Widerspruch einzulegen. Das allgemeine Widerspruchsrecht des Art. 21 DSGVO gilt somit nicht bedingungslos. Räumt der Verantwortliche dem Nutzer hingegen von vornherein ein anlassloses/bedingungsloses Widerspruchsrecht ein, so kann dies erheblich dazu beitragen, dass die Interessenabwägung zugunsten des Verantwortlichen ausfällt.

Beispiel – Reichweitenmessung:

Der Website-Betreiber bindet ein Tool zur Reichweitenmessung ein. Der Nutzer findet in den Datenschutzbestimmungen Hinweise zu einem Opt-Out-Verfahren, das er jederzeit ausführen kann. Hierzu klickt er einen Link an, der zu einem Opt-Out-Verfahren des Anbieters führt. Das Opt-Out-Verfahren wurde vom Website-Betreiber vorab geprüft. Verantwortlich für die Umsetzung des Widerspruchs bleibt der Website-Betreiber, auch wenn der Anbieter des Tools zur Reichweitenmessung ein Opt-Out-Verfahren zur Verfügung stellt. Nach Anklicken des Links wird der Widerspruch unmittelbar umgesetzt. Eine weitere Verarbeitung der Nutzungsdaten für statistische Analysen (Reichweitenmessung) findet nicht mehr statt.

Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, besteht allerdings ohnehin ein Widerspruchsrecht ohne Bedingungen, auch für ein Profiling in Verbindung mit Direktwerbung (Art. 21 Abs. 2 DSGVO). In diesen Fällen wirkt sich das Einräumen des Widerspruchsrechts nicht auf die Interessenabwägung aus. Aus Art. 25 Abs. 2 DSGVO und dem Erwägungsgrund 78 ergibt sich zudem, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, die u. a. sicherstellen, dass durch die Nutzer vorgenommene technische Voreinstellungen an ihren Endgeräten zum Schutz ihrer personenbezogenen Daten (z. B. „Do Not Track“)

auch eingehalten werden. Eine technische Umgehung der gewünschten Voreinstellungen, beispielsweise die Verwendung von Frist-Party-Cookies aufgrund blockierter Third-Party-Cookies, ist nicht zulässig.

c) Verkettung von Daten

Zu berücksichtigen ist, welche Möglichkeiten der Verknüpfung, Vervielfältigung von Datensätzen (z. B. durch eine höhere Anzahl an datenverarbeitenden Akteuren) und Anreicherungen von Datensätzen, insbesondere zweckunabhängig, existieren und welche Risiken für die betroffenen Personen hieraus entstehen.

Auch im Zusammenhang mit der Verkettung von Daten kann es eine Rolle spielen, welche Art von Identifikatoren genutzt werden. Zudem können Verknüpfungen von Nutzungsdaten und Inhaltsdaten (z. B. aus Kundenkonten) ebenso wie die geräteübergreifende Verkettung von Daten risikoerhöhend wirken. Darüber hinaus muss es in die Bewertung einfließen, wenn über Analysetools Dritte als Dienstleister eingebunden werden, die eine Verknüpfung mit eigenen Daten vornehmen oder Daten von verschiedenen Kunden, Websites und Geräten zusammenführen.

Zudem sind diese Verfahren technisch-organisatorisch so zu gestalten, dass ein Personenbezug frühestmöglich beseitigt wird und Nutzungsprofile – wenn überhaupt – unter Pseudonymen erstellt werden. Dies ergibt sich allerdings in der Regel bereits aus den Anforderungen des Art. 5 DSGVO und dessen technisch-organisatorischer Implementierung nach Art. 25 DSGVO, insbesondere Art. 25 Abs. 2 DSGVO (privacy by default).

Diese Anforderungen sind ebenso wie die Erfüllung der Transparenzanforderungen nach Art. 12 ff. DSGVO verpflichtend umzusetzen, so dass diese im Rahmen der Interessenabwägung nicht zugunsten des Verantwortlichen berücksichtigungsfähig sind. Darüber hinaus sind zwingend die Anforderungen aus Art. 24 und 32 DSGVO zu beachten und entsprechende technisch-organisatorische Maßnahmen zu ergreifen.

d) Beteiligte Akteure

Je mehr Verantwortliche, Auftragsverarbeiter und sonstige Empfänger in die Verarbeitungstätigkeit einbezogen sind, desto größer ist die Beeinträchtigung für den Betroffenen. Dies ergibt sich daraus, dass einerseits durch die steigende Anzahl an Akteuren das Risiko einer Datenschutzverletzung steigt. Anderseits sind regelmäßig die Eingriffsmöglichkeiten des Verantwortlichen erschwert, weil die Akteure räumlich entfernt sind und unterschiedlichen Jurisdiktionen unterliegen (z. B. Akteure mit Niederlassungen in unterschied-

lichen Staaten). Dem kann der Verantwortliche entgegensteuern, indem er zusätzliche technische und organisatorische Schutzmaßnahmen ergreift, die über die Mindestanforderungen der Art. 5 Abs. 1 lit. f), Art. 25 und Art. 32 DSGVO hinausgehen.

e) Dauer der Beobachtung

Im Rahmen der Wertungen ist relevant, wie lange die Möglichkeit besteht, die Nutzer wiederzuerkennen und Informationen zum Nutzungsverhalten zu sammeln und zuzuordnen. Relevant ist in diesem Zusammenhang z. B., welche Lebensdauer Cookies haben. Eine sehr kurze Wiedererkennungsphase könnte z. B. auch zur Kompensation in anderen Bereichen führen. Z. B. fällt der Umfang der über den Nutzer erfassten Informationen bei der Interessenabwägung weniger ins Gewicht, je kürzer die Nutzer ausgesondert und wiedererkannt werden können.

f) Datenkategorien

Bei der Bewertung ist zu berücksichtigen, welche Datenkategorien erhoben und in welchem Detaillierungsgrad Informationen erfasst werden (z. B. Protokollierung, auf welche Dateien zugegriffen wurde, Tippverlaufsaufzeichnung, Aufzeichnung des Scrollings, Erhebung von Texten aus angefangenen Formularen, auch wenn diese nicht abgeschickt werden, Suchanfragen etc.). Die Verarbeitung von pseudonymen Daten ist grundsätzlich weniger belastend, da die Identität der betroffenen Person verschleiert wird und somit die Wahrscheinlichkeit geringer ist, dass die betroffene Person durch Dritte identifiziert wird. Daher ist im Rahmen der Interessenabwägung auch zu berücksichtigen, ob die betroffene Person direkt oder indirekt identifizierbar ist.

Zudem spielt es eine Rolle, ob und in welcher Form Nutzungsprofile erstellt werden, insbesondere welche Anzahl von Nutzungsdaten zusammengefügt und ob anschließend ergänzend Interessen und Merkmale zugeordnet werden, um den Nutzer in einer bestimmten Zielgruppe zu verorten und ihn schließlich zielgruppenspezifisch anzusprechen (Profiling z. B. zu Zwecken der Werbung oder personalisierten Information). Diese Form der Profilbildung erfolgt größtenteils dienst- und geräteübergreifend und kann dadurch zu einem umfassenden, tiefgreifenden und langanhaltenden Eingriff in die Privatsphäre des Nutzers führen. Bei einer umfangreichen Verarbeitung entstehen Risiken für die Rechte und Freiheiten der Nutzer, die zu einem physischen, materiellen oder immateriellen Schaden führen könnten. Beispielsweise können die erstellten Nutzungsprofile zu einer Diskriminierung, einem Identitätsdiebstahl, einem finanziellen Verlust, einer Rufschädigung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen. Dieses Risiko ist

höher zu bewerten, wenn bei der Profilbildung persönlichkeitsbeschreibende Aspekte, wie z. B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder das Verhalten analysiert oder prognostiziert werden. Auch die Erstellung von Bewegungsprofilen und -prognosen ist regelmäßig als hohes Risiko einzustufen.

g) Umfang der Datenverarbeitung

Außerdem ist der Umfang der Datenverarbeitung zu berücksichtigen. Dies ergibt sich aus den Art. 24, 25, 32 und 35 DSGVO. Je größer die Menge an verarbeiteten Daten, desto höher ist das Risiko für die Rechte und Freiheiten der betroffenen Person. Je mehr Daten verarbeitet werden, desto größer ist die Gefahr, dass durch Anhäufung großer Datenmengen weitere Informationen zum Vorschein kommen, die diskriminierend oder diffamierend sein können oder z. B. Rückschlüsse auf besondere Kategorien von Daten gem. Art. 9 Abs. 1 DSGVO zulassen. Der Umfang der Datenverarbeitung ist darüber hinaus eng mit der Speicherdauer verbunden. Werden über einen langen Zeitraum permanent Daten hinzugespeichert, vergrößert dies den Umfang der Datenverarbeitung.

Ebenso spielt die Anzahl der betroffenen Personen eine entscheidende Rolle bei der Interessenabwägung. Je größer die Anzahl der betroffenen Personen, desto eher und feingranularer können Vergleichsgruppen gebildet werden. Daraus kann sich ein erhöhtes Diskriminierungspotenzial ergeben und die Gefahr, dass Merkmale ermittelt werden, die ohne Betrachtung der Vergleichsgruppe nicht erkennbar gewesen wären.

Werden personenbezogene Daten verarbeitet, die Rückschlüsse auf besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO zulassen, bedarf es in jedem Fall einer Einwilligung. Hierzu zählen beispielsweise Dating-Portale, Websites von politischen Parteien, religiösen Vereinigungen, Online-Gesundheitsportale oder Webangebote für Erkrankungen. Daher ist in diesen Fällen eine besondere Sorgfalt bei der Einholung der informierten Einwilligung nötig, die alle Aspekte der Datensammlung erläutert, einschließlich des Umstand, dass Informationen über die sexuelle Orientierung oder das Interesse an den jeweiligen politischen Parteien an Dritte weitergegeben werden.

h) Kreis der betroffenen Personen (Kinder und andere schutzbedürftige Personen)

Im Rahmen der Interessenabwägung ist zu berücksichtigen, welche Personen von Verarbeitungsmaßnahmen betroffen sind. Sofern eine erhöhte Schutz-

bedürftigkeit von Personen gegeben ist, führt das dazu, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen höher gewichtet werden. Dies gilt insbesondere für Kinder, die ausdrücklich in Art. 6 Abs. 1 lit. f) DSGVO benannt werden. Darüber hinaus können solche Überlegungen auch eine Rolle spielen, wenn z. B. die Erhebung von Nutzungsdaten und das Profiling von Nutzern gerade auch dazu dient, besondere Anfälligkeiten oder Situationen der Wehrlosigkeit zu erkennen und nutzbar zu machen.

Es ist weiterhin das Verhältnis des Verantwortlichen zur betroffenen Person zu berücksichtigen. So kann es Situationen geben, in denen zwischen dem Verantwortlichen und der betroffenen Person ein Machtungleichgewicht besteht. Dies ist beispielsweise im Beschäftigtenverhältnis der Fall oder wenn der Verantwortliche eine Monopolstellung hat. Besteht das Machtungleichgewicht zugunsten des Verantwortlichen, so führt dies ebenfalls dazu, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen höher zu gewichten sind.

Beispiel:

Der Website-Betreiber bietet eine Beratungsplattform für Suchterkrankte an. Nutzer können auf der Website neben Hinweisen zu Kontaktmöglichkeiten von Beratungsstellen vor Ort auch Informationen zur Erkrankung und Erste Hilfe finden. Der Website-Betreiber bindet eine Vielzahl an Tools von Werbenetzwerken ein, die die Nutzungsdaten der Website-Besucher für eigene Zwecke weiterverarbeiten. Hier besteht ein besonderes Verhältnis zwischen Website-Besucher und -Betreiber. Aufgrund des Informationsangebots können Rückschlüsse auf besondere Kategorien von personenbezogenen Daten gem. Art. 9 Abs. 1 DSGVO gezogen werden. Außerdem ist zu vermuten, dass die Nutzer das Informationsangebot aufgrund eigener Betroffenheit in Anspruch nehmen und daher aufgrund ihres besonderen Interesses an Vertraulichkeit bzw. an einer weitestgehend anonymen Nutzung besonders schützenswert sind.

IV.
Fazit

Verantwortliche sollten sich bewusst machen, dass die Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f) DSGVO eine substanzielle Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten verlangt und auf den konkreten Einzelfall bezogen sein muss. Unzureichende oder pauschale Feststellungen, dass eine Datenverarbeitung gem. Art. 6 Abs. 1 lit. f) DSGVO zulässig sei, erfüllen nicht die gesetzlichen Anforderungen.

Sollte der Verantwortliche zum Ergebnis kommen, dass die Interessenabwägung zugunsten der betroffenen Person ausfällt und keine andere Rechtsgrundlage in Betracht kommt, ist die Datenverarbeitung – falls überhaupt – nur nach voriger informierter Einwilligung (Art. 6 Abs. 1 lit. a) DSGVO) rechtmäßig („jedenfalls dann…“).

Anhang I – Beispiel für eine Interessenabwägung

Beispiel Tracking-Pixel:

Ein Unternehmen (Online-Shop für Medikamente und Kosmetikartikel, im Folgenden: „Unternehmen“) schaltet auf einem sozialen Netzwerk Werbeanzeigen. Um Werbung im sozialen Netzwerk steuern und auswerten zu können, bindet das Unternehmen ein Tracking-Pixel, sog. Zähl-Pixel, des sozialen Netzwerks auf seiner Website des Unternehmens ein. Mithilfe des Pixels werden vom sozialen Netzwerk unmittelbar Daten der Website-Besucher erfasst. Anhand dieser Nutzerdaten erhält das Unternehmen Informationen zur Website. Dazu gehören beispielsweise Angaben darüber, wie der Nutzer auf die Website gelangt, wie er die Website nutzt, wie viele Nutzer sich für Newsletter anmelden und Produkte in den Warenkorb legen. Diese Informationen nutzt das Unternehmen, um die Werbekampagnen auf dem sozialen Netzwerk zu gestalten und Streuverluste zu vermeiden. Um eine Auswertung des Nutzungsverhaltens zu ermöglichen sowie zielgerichtete Werbung zu schalten, verwendet das soziale Netzwerk die Daten des Online-Shops auch für eigene Zwecke und greift auf Daten aus eigenen Quellen zurück.

Das Unternehmen möchte zunächst keine Einwilligung der Nutzer einholen und fragt sich, ob die Datenverarbeitung gem. Art. 6 Abs. 1 lit. f) DSGVO gestützt werden kann.

Bewertung: Rechtmäßigkeit der Verarbeitung

Gemäß Art. 6 Abs. 1 lit. f) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Danach ist eine Abwägung zwischen den Interessen des Unternehmens und den Interessen der betroffenen Personen, d. h. der Kunden des Unternehmens vorzunehmen.

1. Stufe – Berechtigte Interesse des Verantwortlichen ermitteln

Das Interesse des Unternehmens an Werbung in einem sozialen Netzwerk kann als wirtschaftliches Interesse als berechtigt angesehen werden.

2. Stufe – Erforderlichkeit

Die Erforderlichkeit für die Verarbeitung der personenbezogenen Daten wäre gegeben, wenn das beschriebene Verfahren geeignet ist, um die Werbung für das Unternehmen zu optimieren, und alternative, gleich effektive Mittel nicht zur Verfügung ständen.

3.Stufe – Interessen, Grundrecht und Grundfreiheiten der betroffenen Person und Abwägung im Einzelfall

Dem gegenüber stehen die Grundrechte der Nutzer der Unternehmenswebsite auf Achtung ihres Privat- und Familienlebens sowie Schutz personenbezogener Daten gem. Art. 7 und Art. 8 GRCh.

Im Rahmen der Abwägung sind Auswirkungen der gegebenen Verarbeitung nicht nur abstrakt oder hypothetisch zu berücksichtigen, sondern es ist auf die konkreten Auswirkungen auf die einzelne betroffene Person abzustellen. Maßgeblich sind dabei u. a. die o. g. Kriterien:

a. Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit / Transparenz
b. Interventionsmöglichkeiten der betroffenen Personen
c. Verkettung von Daten
d. Beteiligte Akteure
e. Dauer der Beobachtung
f. Datenkategorien
g. Umfang der Datenverarbeitung
h. Kreis der Betroffenen (bspw. besonders schutzbedürftige Personen)

Indem das Pixel auf der Website des Unternehmens eingebunden wird, veranlasst das Unternehmen die Erhebung von Informationen durch das soziale Netzwerk, welche konkreten Nutzer wann die einzelnen Seiten der Website aufrufen. Dadurch erhält das soziale Netzwerk weiteres Zusatzwissen über Websitebesucher, das es ohne Tracking-Pixel nicht erlangen würde. Dieses Zusatzwissen nutzt das soziale Netzwerk wiederum für eigene Werbezwecke, um die Zielgruppen für Werbemaßnahmen zu bestimmen. Dabei wird eine Vielzahl an Nutzungsdaten erhoben, die eine umfangreiche Profilbildung des Nutzers ermöglichen. Diese Informationen werden vom sozialen Netzwerk für

die eigene Profilerstellung über die Nutzer verwendet. Der Website-Besucher kann eingebundene Tracking-Pixel weder ohne weiteres erkennen, noch erwartet er, dass sein Nutzungsverhalten website-übergreifend erfasst und zur Profilbildung durch das soziale Netzwerk verwendet wird.

Nutzer von sozialen Netzwerken erwarten zwar, dass personenbezogenen Daten durch Betreiber sozialer Netzwerke verarbeitet werden, die sie im Rahmen einer aktiven Nutzung direkt auf dem sozialen Netzwerk hinterlassen. Dazu gehören beispielsweise gepostete Fotos und Nachrichten oder das „Liken" von Beiträgen anderer Nutzer. Sie sind sich ggf. auch in allgemeiner Form über die Profilbildung durch Betreiber sozialer Netzwerke im Klaren. Der durchschnittliche Nutzer sozialer Netzwerke erwartet jedoch nicht, dass Websites „unsichtbare" Pixel einbinden, um eine Datenverarbeitung durch Dritte zu veranlassen (Vernünftige Erwartung der betroffenen Personen) und sozialen Netzwerken damit Daten zugeliefert werden, die diese wiederum zur Profilbildung nutzen. In jedem Fall steht dies außerhalb dessen, was Nutzer objektiv vernünftigerweise erwarten müssen, denn solche Datenerfassungen durch Dritte wirken sich nur nachteilig auf die Möglichkeit der Nutzer aus, die Verwendung eigener Daten zu kontrollieren und darüber zu bestimmen.

Darüber hinaus hat der Nutzer keine Möglichkeit, der Datenverarbeitung zu widersprechen oder durch sonstige Weise zum Ausdruck zu bringen, dass er die Profilbildung durch einen Dritten nicht wünscht (Keine Interventionsmöglichkeiten). Auch wenn ein Widerspruchsrecht zur Verfügung stünde, würde die Intervention erst nach der Datenverarbeitung möglich werden und käme damit zu spät, um im Hinblick auf die Eingriffsintensität die erforderliche Schutzwirkung zu entfalten.

Bei der Profilbildung werden nicht nur die Nutzungsdaten über einen längeren Zeitraum gespeichert. Anhand der Nutzungsdaten ermittelt das soziale Netzwerk Merkmale und Interessen des Nutzers, um ihn anschließend Zielgruppen zuzuordnen. Dies erfolgt nicht nur auf der Website des o. g. Unternehmens. Da eine Vielzahl von Websites das Pixel einbinden, können die Daten der Nutzer website- und sogar geräteübergreifend erfasst werden. Der Nutzer kann das Ausmaß der Datenverarbeitung nicht mehr erfassen und ist auch nicht in der Lage zu bestimmen, wer und in welchem Umfang seine Daten verarbeitet (Verkettung von Daten, Beteiligte Akteure, Transparenz).

Da das Unternehmen einen Online-Shop für Medikamente betreibt, ist nicht auszuschließen, dass die Nutzer Produkte in den Warenkorb legen oder sich für Artikel interessieren, die Rückschlüsse auf den Gesundheitszustand zulassen. Hier ist bereits fraglich, ob die Rechtsgrundlagen des Art. 6 Abs. 1 DSGVO überhaupt in Betracht kommen können. Fließen diese schützenswerten In-

formationen in das Nutzungsprofil ein, steigt das Risiko für die betroffenen Personen (Datenkategorien, Kreis der betroffenen Personen) in jedem Fall.

Eine Abwägung der o. g. Interessen im konkreten Einzelfall ergibt, dass die Interessen der betroffenen Personen die Interessen des Unternehmens überwiegen und folglich die Einbindung des Pixels nicht gem. Art. 6 Abs. 1 lit. f) DSGVO zulässig ist. Als Rechtsgrundlage käme dann – wenn überhaupt – nur die Einwilligung in Betracht.

3.8
Positionspapier zur biometrischen Analyse

Version 1.0, Stand: 3. April 2019

Beschlossen von der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. und 4. April 2019 gegen die Stimmen Bayerns und Baden-Württembergs.

Inhaltsübersicht

1
Ziel des Positionspapiers

Der Einsatz moderner optisch-elektronischer Verfahren ist ein weiterer Baustein für eine immer umfassendere Profilbildung von Personen im Alltag. Anhand von Videoaufnahmen und der Auswertung des Gesichts einer Person können deren Alter und Geschlecht recht zuverlässig bestimmt werden. Durch Analyse der Mimik sind zusätzlich auch Rückschlüsse auf die Gefühlslage eines Menschen möglich (Emotional Decoding). All dies kann technisch ohne Wissen und Einverständnis der Betroffenen erfolgen. Derartige Verfahren werden beispielsweise verwendet, um die Wirksamkeit von Werbung zu messen und genauer auf die gewünschten Zielgruppen zuschneiden zu können.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat den Arbeitskreis „Technische und organisatorische Datenschutzfragen“ damit beauftragt, sich gemeinsam mit dem Arbeitskreis „Videoüberwachung“ mit dem Thema Verarbeitung von Daten durch Sensorik und Videotechnik und deren datenschutzrechtliche Einordnung zu befassen. Ziel ist es, die Leistungsfähigkeit von biometrischen Sensoren einschließlich Videokameras und der dazu gehörigen Verarbeitungssysteme zu ermitteln sowie Verarbeitungsziele und -prozesse zu beschreiben. Anschließend werden diese Elemente rechtlich bewertet und Empfehlungen zur Gestaltung von Verfahren abgeleitet.

2
Grundlagen der biometrischen Erkennung

2.1
Begriffsbestimmungen

Die Begriffe und Definitionen sind Übersetzungen aus dem ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV), wie es in der SC37 Working Group 1 für den internationalen Standard ISO/IEC 2382-37 erarbeitet wurde.

– *Anonymisierter biometrischer Datensatz*

  Biometrischer Datensatz, der bewusst von personenbezogenen Metadaten entkoppelt wurde

– *Betroffene Person*

  Individuum, dessen individualisierte biometrische Daten sich innerhalb des biometrischen Systems befinden

– *Biometrische Anwendungs-Datenbank*

  Datenbank aus biometrischen Daten und zugeordneten Metadaten, die durch den Betrieb einer biometrischen Anwendung erzeugt wurden und diese unterstützen sollen

– *Biometrisches Charakteristikum*

  Biologisches oder verhaltensabhängiges Charakteristikum eines Individuums, von welchem sich zur Unterscheidung verwendbare, reproduzierbare biometrische Merkmale ableiten lassen, die zum Zwecke der biometrischen Erkennung einsetzbar sind

– *Biometrische Daten*[28]

  Biometrisches Sample oder Ansammlung biometrischer Samples in jeder Verarbeitungsstufe, biometrische Referenzen, biometrische Probe, biometrisches Merkmal oder biometrische Eigenschaften

28 Die Definition weicht von der Begriffsbestimmung aus Art. 4 Ziffer 14 DS-GVO ab; siehe auch Abschnitt 6.1 Begriff der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO. Art. 14. Ziffer 14 lautet: „Biometrische Daten“ (*sind*) mit speziellen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

– *Biometrisches Enrolment*

  Vorgang der Erzeugung und Speicherung eines biometrischen Enrolmentdatensatzes in Übereinstimmung mit den Enrolmentregeln

– *Biometrische Enrolmentdatenbank*

  Datenbank aus biometrischen Enrolmentdatensätzen[29]

– *Biometrischer Enrolmentdatensatz*

  Datensatz, der sich auf eine betroffene Person bezieht, nichtbiometrische Daten enthält und mit einem biometrischen Referenz-Identifikator assoziiert ist

– *Biometrisches Erfassungsgerät*

  Gerät, das in der Lage ist, aus einem biometrischen Charakteristikum ein Signal zu sammeln und in ein erfasstes biometrisches Sample zu konvertieren

– *Biometrisches Erfassungsteilsystem*

  biometrisches Erfassungsgerät(e) und zugehörige Teilprozesse, die für die Durchführung eines biometrischen Erfassungsprozesses notwendig sind

– *Biometrische Erkennun*g

  Automatisierte Erkennung von Individuen anhand ihrer verhaltensbezogenen und biologischen Charakteristika

– *Biometrische Identifikation*

  Prozess, um bei der Suche in einer biometrischen Enrolmentdatenbank den Identifikator einer biometrischen Referenz, der einem einzigen Individuum zugeordnet werden kann, zu finden

29 Eine Datenbank mit biometrischen Daten, die nicht einer betroffenen Person zugeordnet werden können, ist eine biometrische Datenbank, aber keine biometrische Enrolmentdatenbank. Eine biometrische Enrolmentdatenbank kann die biometrische Referenzdatenbank enthalten, muss aber nicht. Eine Trennung der Datenbanken kann aus Gründen der Sicherheit, des Datenschutzes, der Rechtslage, der Systemarchitektur oder der Erkennungsleistung erforderlich sein.

– *Biometrische Verifikation*[30]

  Prozess, eine biometrische Behauptung durch einen biometrischen Vergleich zu bestätigen

– *Biometrisches Merkmal*

  Zahlen oder Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden

– *Biometrische Merkmalsextraktion*

  Auf ein biometrisches Sample angewendeter Prozess mit dem Ziel, Zahlen und markante Kennzeichen wiederholbar zu isolieren und auszugeben, die mit anderen Zahlen und markanten Kennzeichen, die aus anderen biometrischen Samples gewonnen wurden, vergleichbar sind

– *Biometrische Probe*

  Biometrische Samples oder biometrische Merkmale, die als Eingabe zu einem Algorithmus zum Vergleich mit einer biometrischen Referenz dienen

– *Biometrische Referenz*

  ein oder mehrere gespeicherte biometrische Samples, biometrische Templates oder biometrische Modelle, die einer betroffenen Person zugeordnet wurden und als Objekt zum biometrischen Vergleich verwendet werden

– *Biometrische Referenz-Datenbank*

  Datenbank mit biometrischen Referenzdatensätzen

– *Biometrisches Sample*

  Analoge oder digitale Repräsentation biometrischer Charakteristika vor der biometrischen Merkmalsextraktion

---

30 Der Begriff der *biometrischen Authentifikation* wurde im Prozess der Standardisierung von ISO/IEC 2382-37 als veraltet abgelehnt. Der Begriff *Authentisierung* wird in diesem Papier deshalb so verwendet, wie vom Bundesamt in der Sicherheit der Informationstechnik im Glossar des IT-Grundschutz-Kompendiums definiert (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html): „Authentisierung bezeichnet den Nachweis oder die Überprüfung der Authentizität. Die Authentisierung einer Identität kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen. Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen."

– *Biometrisches System*

  System zum Zwecke der biometrischen Erkennung von Individuen anhand ihrer verhaltensbezogenen und biologischen Charakteristika[31]

– *Biometrisches Identifikationssystem*

  System zum Zwecke der biometrischen Identifikation

– *Biometrisches Template (Synonym: Referenz-Merkmalsvektor)*

  Menge von gespeicherten biometrischen Merkmalen, die direkt vergleichbar zu den biometrischen Merkmalen einer biometrischen Probe sind

– *Enrolen (registrieren)*

  Erstellen und Speichern eines biometrischen Enrolmentdatensatzes in Übereinstimmung mit einer biometrischen Enrolmentregel

– *Nichtauthentische Person*

  Biometrisch subversive zu erfassende betroffene Person, die versucht, mit der biometrischen Referenz einer anderen Person Übereinstimmung zu erlangen

– *Nicht identifizierte biometrische Daten*

  biometrische Daten, deren betroffene Person derzeit nicht bekannt ist

– *Präsentation, bewusste*

  Präsentation unter dem Bewusstsein der zu erfassenden betroffenen Person

– *Präsentation, kooperative*

  Präsentation durch eine kooperative zu erfassende betroffene Person

– *Präsentation, indifferente*

  Präsentation, bei der die zu erfassende betroffene Person sich des durchgeführten biometrischen Erfassungsprozesses nicht bewusst ist

– *Präsentation, unkooperative*

  Präsentation einer unkooperativen zu erfassenden betroffenen Person

31 Ein biometrisches System enthält biometrische und nichtbiometrische Komponenten.

– *Verdecker einer Identität*

  Subversive zu erfassende betroffene Person, die versucht, sich einer Übereinstimmungsentscheidung mit der eigenen biometrischen Referenz zu entziehen

– *Vergleich*

  Schätzung, Berechnung oder Messung der Ähnlichkeit oder Unterschiedlichkeit zwischen der biometrischen Probe und biometrischen Referenzen

2.2 Funktionsweise der biometrischen Erkennung

2.2.1 Allgemeine Beschreibung

Verfahren zur biometrischen Erkennung sind immer Teil eines umfassenderen biometrischen Systems. Mit der biometrischen Erkennung soll festgestellt werden, ob ein gegenüber einem biometrischen Erfassungssystem präsentiertes biometrisches Charakteristikum mit einer bekannten biometrischen Referenz übereinstimmt. Beispiele für biometrische Systeme sind in Kapitel 5 dargestellt. Dabei kann festgestellt werden, ob eine Person bekannt ist, d. h. ob biometrische Daten von ihr vorliegen, oder ob sogar weitergehende Daten wie Name, Adresse usw. bekannt sind. Abhängig vom Ergebnis der Prüfung wird dann in dem System fortgefahren.

Bei der biometrischen Erkennung können drei Phasen unterschieden werden:

In der initialen Phase werden die biometrischen Charakteristika erstmalig erfasst, Merkmale berechnet und Referenzen gespeichert. Im Falle eines Enrolments werden diese biometrischen Daten mit weiteren Daten verknüpft.

Das eigentliche (Wieder-)Erkennen findet im Rahmen des biometrischen Systems statt, wenn nach erneutem Erfassen der biometrischen Charakteristika die Merkmale errechnet werden und im Vergleich mit den vorhandenen Referenzdaten festgestellt wird, ob die Person bekannt ist.

Die abschließende Phase ist das Löschen des biometrischen Merkmals und der zugehörigen Daten.

2.2.2 Enrolment

Grundsätzlich müssen als Ergebnis der ersten Phase die Referenzwerte gewonnen werden. Dies geschieht, indem biometrische Samples gewonnen

sowie Merkmale errechnet werden, die bei einem Enrolment um weitere Daten ergänzt und dann in einer Referenzdatenbank gespeichert werden.

Üblicherweise wird in dieser Phase einem Erfassungsgerät (vgl. hierzu Abschnitt 3) ein zu einer Person gehörendes biometrisches Charakteristikum präsentiert. Daraus wird ein Sample oder ein Template generiert und in einer dezentralen Datenbank, beispielsweise dem Zutrittskontrollsystem der Niederlassung eines Verantwortlichen, einer zentralen Datenbank eines Verantwortlichen oder sogar übergreifend für mehrere Verantwortliche, wie im Bereich der Polizei, gespeichert. Weiterhin gibt es Systeme, bei denen die biometrischen Daten auf einem Datenträger (Chipkarte) gespeichert werden, der sich im Besitz der betroffenen Person befindet. Zusätzlich zu den biometrischen Daten werden noch Angaben zu der Person gespeichert. Bei Reisedokumenten wird als Sample ein Bild des Fingerabdrucks erstellt und dieses Bild wird (signiert) auf einem Chip des Dokuments gespeichert. Es gibt auch Entwicklungen, Templates zusätzlich zu einer reinen Zugriffskontrolle dergestalt zu schützen, dass sie nur in einem bestimmten System genutzt werden können (Biometric Template Protection).

Der Umfang der Daten, die zur Person gespeichert werden, kann abhängig von der Anwendung erheblich voneinander abweichen; siehe hierzu die verschiedenen Szenarien aus Kapitel 5.

Beim Enrolment kann es Fehler geben, die als FTE (Failure to Enrol Rate) bezeichnet werden; beispielsweise gibt es beim biometrischen Merkmal „Fingerabdruck“ Personen, deren Fingerabdrücke nicht genug ausgeprägt sind und daher nicht erfasst werden können.

Unabhängig von diesen sehr technischen Aspekten ist auch relevant, ob das Erfassen der Daten ohne Wissen des Betroffenen (wie etwa bei der Suche nach Straftätern, von denen nur ein biometrisches Merkmal bekannt ist), mit Wissen (wie bei einem Hinweis auf die Nutzung von Videotechnik) oder durch eine bewusste Präsentation des Betroffenen (wie bei Zutrittskontrollsystemen) stattfindet.

2.2.3
Prüfung auf Übereinstimmung

Nach der Erfassung, in der Regel also dem Enrolment, stehen die Referenzwerte zur Verfügung. Wenn im Rahmen des biometrischen Systems einem Erfassungsgerät ein biometrisches Charakteristikum präsentiert wird, werden daraus die Merkmale generiert. Diese werden mit den Merkmalen verglichen, die sich aus den Daten der Referenzdatenbank bzw. aus der

vorgelegten Chipkarte ergeben. Das Ergebnis des Vergleichs wird in Form eines Prozentsatzes ausgegeben.

Es muss daher bei der Konfiguration des Verfahrens ein Schwellwert festgelegt worden sein, ab dem eine Übereinstimmung zwischen den Referenzen und dem gerade errechneten Wert angenommen wird. In Folge dieser systemisch bedingten Unschärfe gibt es Fälle, in denen eine Übereinstimmung angenommen wird, obwohl sie nicht vorlag (FAR: False Acceptance Rate), und es gibt Fälle, in denen eine Person nicht erkannt wurde (FRR: False Rejection Rate). Abhängig von der Anwendung muss der Schwellwert gesetzt werden und daraus ergeben sich FAR und FRR. Beispielsweise wird man bei einem Zutrittskontrollsystem zu einem Hochsicherheitstrakt einen unbefugten Zutritt mit hoher Wahrscheinlichkeit verhindern wollen, weshalb der Schwellwert hoch gesetzt wird. Damit sinkt die FAR. Gleichzeitig steigt die FRR, d. h. es wird mehr Fälle geben, in denen eine eigentlich berechtigte Person am Zutritt gehindert wird.

Abhängig vom genutzten biometrischen Charakteristikum kann die Kooperation der betroffenen Person beim Enrolment und beim Abgleich erforderlich sein oder nicht. Während beispielsweise ein Foto problemlos ohne Wissen und Kooperation des Betroffenen erstellt werden kann, muss bei einem Handvenenscanner die Person ihre Handfläche auf den Sensor auflegen. Der Fingerabdruck kann oft sogar noch nachträglich an Orten, an denen sich die betroffene Person aufgehalten hat, abgenommen und gegenüber dem Verfahren präsentiert werden.

2.2.4
Widerstand gegen Verfälschungen

Ein weiterer zu betrachtender Bereich ist das Umgehen des Verfahrens. Das können Verdecker einer Identität sein oder nichtauthentische Personen, d. h. Personen, die gefälschte biometrische Charakteristika präsentieren. Stichwörter sind hier Lebenderkennung und Nicht-Fälschbarkeit. Gerade biometrische Verfahren, bei denen die Kooperation des Betroffenen für das Erfassen des Charakteristikums nicht erforderlich ist, sind anfällig. Ob und inwieweit sich daraus datenschutzrelevante Risiken ergeben, kann nur anhand der gesamten Anwendung beurteilt werden. So kann es erhebliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben, wenn durch die Präsentation gefälschter Charakteristika eine fremde Identität angenommen werden kann.

3.
Systeme zur Erfassung biometrischer Charakteristika

Es existiert bereits eine große Anzahl von technischen Systemen, bei denen biometrische Charakteristika ein zentraler Bestandteil der Verarbeitung sind. Biometrische Systeme, deren Zweck die biometrische Erkennung von Individuen durch biometrische Charakteristika ist, lassen sich anhand der folgenden Kriterien systematisieren:

– Welche konkreten biometrischen Charakteristika werden in dem jeweiligen System verwendet (biologische Charakteristika, siehe Kapitel 3.1, und verhaltensabhängige Charakteristika sowie medizinische Daten als spezielle Untergruppe der biologischen Charakteristika)?
– Mit Hilfe welcher Sensoren, die Teil eines biometrischen Erfassungsgeräts sind, werden die biometrischen Charakteristika erfasst (optische, akustische oder sonstige Sensoren, siehe Kapitel 4)?
– Zu welchem Zweck wird die Verarbeitung der biometrischen Charakteristika durchgeführt?

Es ist davon auszugehen, dass die Anzahl dieser Systeme sowie die Integration der Systeme in komplexe Anwendungen in den nächsten Jahren deutlich an Bedeutung gewinnen werden, da

– die Nutzer bereit sind, diese Systeme zu verwenden (z. B. Nutzung von Wearables zur Aktivitätsmessung, Entsperrung von Smartphones durch Fingerabdruck oder Gesichtserkennung),
– die Integration von Sensoren in digitale Infrastrukturen zunimmt (z. B. Kontaktlinsen, die Blutzuckerwerte messen und übermitteln können) und
– innovative, neue Geschäftsmodelle entwickelt werden, die biologische Eigenschaften verwenden (z. B. Versicherungstarife für „gesunde“ Menschen).

Nicht jedes biometrische Charakteristikum kann allerdings für jeden Zweck verwendet werden.

So werden für die Identifikation oder die Verifikation biometrische Charakteristika benötigt, die „statisch“ sind oder sich nur sehr schwer (z. B. durch plastische Chirurgie) verändern lassen (z. B. Gesicht, Fingerabdruck, Stimme oder das menschliche Genom).

Für Geschäftsmodelle, deren Schwerpunkte vertriebsorientiert sind (Werbung oder Produkte für Personen, die spezielle biologische Eigenschaften aufweisen), werden biologische Eigenschaften verwendet, die „dynamisch“ sind (z. B. Blutdruck, Gewicht), die sich also im Zeitablauf ändern können. Damit können z. B. Zielgruppen definiert und wirtschaftlich erschlossen werden. So ist es

möglich, durch ein bestimmtes Verhalten (z. B. Kauf und Verwendung eines Produktes) eine Veränderung dieser biologischen Eigenschaft zu bewirken.

3.1
Erfassung biometrischer Charakteristika

3.1.1
Fingerabdruck/Finger-Bild

Der Fingerabdruck ist ein Abdruck der Papillarleisten am Endglied eines Fingers (Fingerkuppe bzw. Fingerbeere). Da bisher keine zwei Menschen mit dem gleichen Fingerabdruck bekannt sind, geht man von der Einzigartigkeit des Fingerabdrucks aus. Biologisch gesehen ist eine Papillarleiste eine Erhöhung der Epidermis auf der Handfläche oder der Fußsohle. In sehr seltenen Fällen fehlen den Fingern infolge eines genetischen Defekts die Papillarleisten und sie hinterlassen damit keine Abdrücke. Ein vergleichbares Phänomen kann bei Personen auftreten, deren Finger bei der Arbeit oder im Sport stark belastet werden; Beispiele sind Fliesenleger oder Handballer.

Es werden folgende Charakteristika des Fingerabdrucks unterschieden: Grundmuster, grobe Merkmale, feinere Merkmale (Minuzien) und Porenstruktur.

Anhand dieser Charakteristika und ihrer Verteilung innerhalb eines Fingerabdrucks kann eine einzigartige Unterscheidbarkeit gewährleistet werden.

Zur Extrahierung der Minuzien wird ein spezieller Algorithmus verwendet, durch den die Minuzien in eine mathematische Form gebracht werden. Aus dem vom Fingerabdruckscanner gelieferten Bild werden für jeden Fingerabdruck spezifische Daten gesammelt, die zum Einlernen oder späteren Vergleich mit bestehenden Fingerabdruckdaten ausreichen. Ein konkreter Fingerabdruck ist aus den Minuziendaten nicht mehr rekonstruierbar.[32] Es könnte aber ein Fingerabdruck erstellt werden, der ein identisches Template bei einer Prüfung liefert.

3.1.2
Iris

Die Iris ist Teil des menschlichen Auges. Bei der Iris-Erkennung wird über eine Kamera das Farbmuster der Iris erfasst und nach bestimmten Merkmalen (Punkte, Sprenkel, Streifen, Fäden) bewertet.

32 Quelle: https://de.wikipedia.org/wiki/Fingerabdruck

Zwischen der Iris (Regenbogenhaut) und der Hornhaut des menschlichen Auges liegen komplexe band- und kammartige Bindegewebsstrukturen. Diese Strukturen sind bei jedem Menschen unterschiedlich. Sie unterscheiden sich selbst bei eineiigen Zwillingen. Außerdem verändern sie sich in einem gesunden Auge während eines Lebens wenig. Das mit einer herkömmlichen Kamera (z. B. einer CCD-Kamera[33]) von außen aufgenommen Bild der Iris lässt diese Strukturen erkennen und eignet sich damit als biologisches Charakteristikum.

Bei Menschen mit dunkler Augenfärbung sind die Strukturen im sichtbaren Licht allerdings nur schwer zu erkennen. Biometrische Iriserkennungssysteme beleuchten daher die Iris aus einem Abstand von etwa einem Meter mit für das Auge nahezu unsichtbarem Licht im nahen Infrarotbereich. Dieses durchdringt den „Farbstoff" des menschlichen Auges (Melanin) besser als sichtbares Licht. So kann eine Aufnahme der Irisstrukturen bei allen Menschen mit gesunden Augen angefertigt werden, ohne zu blenden. Aus den aufgenommenen Bildern wird mit speziell für diesen Zweck entwickelten mathematischen Methoden ein eindeutiger Datensatz gebildet, der als Basis für die biometrische Erkennung dient.[34]

3.1.3
Netzhaut (Retina)

Die Retina ist, ebenso wie die Iris, Teil des menschlichen Auges und bezeichnet die Anordnung der Blutgefäße in bzw. hinter der Netzhaut. Die Blutgefäße im Augenhintergrund bilden ein Muster. Durch die Reflexion des eingestrahlten Lichtes an der Retina entsteht ein charakteristisches Gebilde, das von einer Kamera aufgenommen werden kann.[35]

Die Retina ist durch Verteilung, Form und Muster ihrer Blutgefäße individuell eindeutig charakterisiert. Da das exakte Muster der Blutgefäße nicht nur durch genetische Faktoren festgelegt wird, lassen sich selbst eineiige Zwillinge anhand ihrer Retina unterscheiden. Ebenso wie das Irismuster bleibt das Adernmuster der Netzhaut im Verlauf des Lebens weitgehend konstant und macht dadurch die Retina zu einem sehr beständigen Erkennungsmerkmal. Beeinträchtigt werden kann das Muster der Blutgefäße aber durch Krank-

33 CCD: charge coupled device (ladungsgekoppeltes Bauelement), bezeichnet eine Form von Bildsensoren

34 Quelle: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Iriserkennung/iriserkennung_node.html

35 Ottenberg, Retinaerkennungssysteme, S. 1, abrufbar unter https://www2.informatik.huberlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/retina.pdf

heiten oder Verletzungen, die dann das Bild der Retina vorübergehend oder andauernd verändern. Zu diesen Krankheiten zählen zum Beispiel Diabetes oder eine Degeneration der Macula sowie bedingt durch Bluthochdruck geplatzte Kapillargefäße.[36]

Bei der Retina-Erkennung wird der Augenhintergrund einer Person mit Hilfe eines Infrarot-Lichtes sichtbar gemacht. Im Gegensatz zur Iriserkennung, bei der eine herkömmliche Kamera verwendet werden kann, muss bei der Retinaerkennung der Kopf in eine bestimmte Position zum Erfassungsgerät gebracht werden.

3.1.4
Gesicht

Bei der biometrischen Erkennung des Gesichts werden die biologischen Charakteristika der Gesichtszüge anhand eines digitalisierten Bildes, das mit einer Kamera aufgenommen wurde, bestimmt.

Verwendet werden vor allem solche Charakteristika des Gesichts, die sich aufgrund der Mimik nicht ständig verändern, also obere Kanten der Augenhöhlen, die Gebiete um die Wangenknochen und die Seitenpartien des Mundes. Grundsätzlich erfolgt ein Vergleich der Charakteristika mit der entsprechenden biometrischen Referenz mittels klassischer Bildverarbeitungs- und Bildanalyseverfahren, wie etwa nach Lokalisierung der Augen die Berechnung der Gesichtsmerkmale anhand eines Gitternetzes, das über das Gesicht gelegt wird.[37]

3.1.5
Handgeometrie

Jede menschliche Hand ist einzigartig. Ab einem Alter von etwa 20 Jahren sind die Veränderungen an der menschlichen Hand meist nur noch gering. Für die biometrische Erkennung der Handgeometrie wird ein Bild der Hand (im Lesegerät, gespiegelt von einer Kamera) von oben und seitlich aufgenommen.

Aus diesen Bildern werden die Konturen der Hand erzeugt. Daraus werden dann verschiedene biologischen Merkmale extrahiert und ermittelt, z. B. Werte für Dicke, Länge, Breite und Fläche der Hand bzw. der Finger, die Fingerspitzen und Punkte zwischen den Fingern, Handbreite, Abstände und

36 Ottenberg, a. a. O., S. 2

37 Quelle: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html

Winkel zwischen verschiedenen Interfinger-Points, Fingerkrümmung und Höhe der Handfläche und Finger.

3.1.6
Venenmuster

Die Venenmuster der menschlichen Hand sind komplex und die Position der Venen ist bei jedem Menschen unterschiedlich und bleibt zeitlebens unverändert, sofern die Hand nicht verletzt wird.

Bei der Erkennung der Venenmuster können entweder die Venen der Handinnenfläche, die Venen des Handrückens oder die Fingervenen mit einem Handvenenerkennungs-Sensor erfasst und zur Identifikation genutzt werden. Dazu sendet der Sensor mittels Infrarot-LEDs Nah-Infrarotstrahlung in Richtung der Handflächen aus. Das sauerstoffreduzierte Blut in den Venen absorbiert diese Infrarotstrahlung mehr als das umgebende Gewebe. Damit kann ein eindeutiges Bild der Venen der Hand/des Fingers aufgenommen und für die Erkennung verwendet werden. Die Venen befinden sich vor Missbrauch und Manipulationen gut geschützt innerhalb des Körpers; für das menschliche Auge sind die Merkmale nicht sichtbar. Hautverunreinigungen oder oberflächliche Verletzungen haben keinen Einfluss.

Handvenenerkennung der Handinnenfläche

Bei diesem Verfahren der Erkennung wird das Venenmuster der Handinnenfläche erfasst und mit späteren Aufnahmen verglichen. Für die Identifikation einer Person muss diese ihre Handinnenfläche flach vor den Sensor des Handvenenscanners platzieren, ohne diesen zu berühren (berührungslose Erfassung). Die Erkennungsrate wird bei dem Verfahren derzeit mit nahezu 100 %, die FAR mit 0,000 08 %, die FRR mit 0,01 % angegeben. Dieses ist somit erheblich genauer als z. B. die Fingerabdruckerkennung.

Einsatzgebiete dieses Verfahrens sind elektronischen Zutrittskontrollen für Bereiche, die die höchste Sicherheit verlangen, wie z. B. Rechenzentren, Kraftwerksbereiche, Sperrzonen auf Flughäfen u. v. m., aber auch als Zugangsschutz bei Rechnern. In einigen Ländern (z. B. Japan) wird das System bereits in Bankautomaten für den sicheren Zahlungsverkehr verwendet.

Die Venenerkennung der Handinnenfläche galt als eines der sichersten Verfahren mit extrem hoher Genauigkeit in der Biometrie bis Dezember 2018, dann wurde öffentlich, dass das System mit entsprechender Technik überlistbar ist. Ein Einsatz unter organisatorisch abgesicherten Bedingungen und mit einer Zwei-Faktor-Authentisierung ist dennoch möglich. Des Weiteren können Lasersysteme für die Blutflusserkennung (Lebenderkennung) zusätzlich

als Schutz eingesetzt werden. Bezüglich der Sicherheit bei Geldautomaten werden weitergehende Überlegungen stattfinden müssen, um von einer gesicherten Anwendung ausgehen zu können.

Handrückenvenenerkennung, Fingervenenerkennung

Bei der Handrückenvenenerkennung wird der Handrücken durch den Sensor eingescannt. Während bei der Handinnenfläche Pigmentflecken oder Haare keine Rolle spielen, kann es beim Handrücken zwangsläufig zu entsprechenden Störungen kommen. Ebenso sind Terminals meist so gebaut, dass ein Griff umfasst werden muss und der Handrücken gegen den Sensor gedrückt wird, wodurch kein berührungsloses Verfahren gegeben ist.

Bei der Fingervenenerkennung wird der Finger von der Oberseite sowie der linken und rechten Seite beleuchtet und das Venenmuster von unten eingescannt. Das Venenmuster eines Fingers ist kleiner und weniger komplex als das Muster der Handfläche. Hinzu kommt die größere Empfindlichkeit der Fingervenen bei Kälte. Bei kalten Fingern können sich die Kapillar-Venen komplett zusammenziehen, so dass sie eventuell nicht mehr erkannt werden. Die Fingervenenerkennung erfolgt nicht kontaktlos, da der entsprechende Finger komplett auf dem Sensor aufliegen muss.

Zusammenfassend kann bezüglich der Handrückenvenenerkennung und Fingervenenerkennung gesagt werden, dass sie aufgrund der Störanfälligkeit vernachlässigbar und kaum im Einsatz sind.

4.
Biometrische Sensoren

Ein biometrisches Erkennungssystem setzt sich im Wesentlichen aus den Komponenten Sensor (Messwertaufnehmer), Merkmalsextraktion und Merkmalsvergleich zusammen. Welche Arten von Sensoren zum Einsatz kommen, hängt stark vom biometrischen Charakteristikum ab.

Die Sensorkomponente liefert als Ergebnis ein biometrisches Sample. Die Merkmalsextraktion entfernt mittels Bild- bzw. Datenverarbeitung und -analyse alle vom Sensor gelieferten Informationen, die nicht die geforderten Merkmalseigenschaften erfüllen, und liefert als Ergebnis die biometrischen Merkmale. Durch die fest definierte Verkettung der Merkmale entstehen anschließend sogenannte Templates, die keine Rückschlüsse auf die eigentlichen Rohdaten zulassen. Als dauerhafter Speicher kommen in der Regel zentrale Datenbanken zum Einsatz, meist verbleiben im Gerät daher keine weiteren Daten.

Der Merkmalsvergleicher errechnet schließlich einen Vergleichswert (Ähnlichkeitswert; Score) zwischen dem in der Einlernphase erhaltenen oder aus einer externen Datenbank gespeicherten biometrischen Template und dem aktuellen, von der Merkmalsextraktion gelieferten Datensatz. Überschreitet dieser Vergleichswert eine Schwelle, gilt die Erkennung als erfolgreich. Unter Leistungskriterien versteht man, dass die vom biometrischen Sensor gelieferten Samples statistischen Schwankungen unterliegen, die Falscherkennungen bedingen. Die Zuverlässigkeit wird hauptsächlich nach zwei Kriterien beurteilt: nach der Zulassungsrate Unberechtigter (FAR) und nach der Abweisungsrate Berechtigter (FRR).[38] Sämtliche biometrische Verfahren arbeiten nicht fehlerfrei. Sie liefern nur Wahrscheinlichkeitsaussagen über den Grad an Übereinstimmung von aktuell gemessenen und gespeicherten biometrischen Templates.

Aufgrund der Komplexität des Themas Biometrie beschränkt sich dieses Positionspapier im Weiteren auf solche Systeme, die biometrische Merkmale erzeugen, indem sie die entsprechenden biometrischen Charakteristika einer betroffenen Person auf Basis optischer Sensoren abbilden. Sollten diese Systeme darüber hinaus üblicherweise auch andere Sensoren wie akustische oder haptische Sensoren beinhalten, so wird für die folgenden Systeme nur die optische Komponente betrachtet.

4.1
Videokameras

Videokameras sind Geräte zur Aufnahme von Bildfolgen in elektrischen Signalen. Im Gegensatz zu Filmkameras lassen sich die gespeicherten Bildsignale direkt sichtbar machen, da nicht erst Filme entwickelt werden müssen. Moderne digitale Videokameras setzen in der Regel auf einen CCD-Chip als Bildaufnehmer. Je größer die Fläche des Bildsensors einer Kamera ist, desto mehr Licht kann sie erfassen. Die Lichtempfindlichkeit steigt und das sogenannte Bildrauschen wird verringert.

Aufgrund der weiten Verbreitung von Videokameras, Smartphones und Webcams führen die damit ermöglichten biometrischen Auswertungen zu einer schnellen technischen Weiterentwicklung in diesem Bereich: Die Gesichtserkennung ist aktuell eine der besonders weit fortgeschrittenen Formen der biometrischen Analyse. Hierbei wird zwischen Verfahren in 2D und 3D unterschieden, wobei 3D-Verfahren genauere Erkennungen sowie Überwindungssicherheiten leisten sollen, so dass die Gesichtserfassung der Systeme nicht mehr manipulierbar ist.

38 https://de.wikipedia.org/wiki/Biometrie

Bei der biometrischen Gesichtserkennung wird das Gesicht einer Person mit einer Kamera aufgenommen und anschließend mit einem oder mehreren zuvor gespeicherten Gesichtsbildern verglichen. Liefert die Kamera analoge Werte des Gesichtsbildes, werden diese in digitale Formate umgewandelt (digitalisiert). Die Erkennungssoftware lokalisiert das Gesicht und berechnet seine charakteristischen Eigenschaften. Das Ergebnis dieser Berechnungen, das sog. Template, wird mit den Templates der zuvor gespeicherten Gesichtsbilder verglichen.[39]

Der Prozess beim Einsatz von Videokameras zur Gesichtserkennung lässt sich folgendermaßen schematisch darstellen:[40]

– Bilderfassung
– Lokalisierung des Gesichts
– Lokalisierung der Augen und weiterer Gesichtsbereiche
– Normalisierung des Gesichts
– Merkmalsextraktion
– Templateerstellung

Das Bild des Gesichts einer Person wird mittels einer Kamera im aktuellen Umfeld aufgenommen oder in Form eines Scans eines bereits vorhandenen Bildes der Person erfasst. Der nächste Schritt besteht aus einer Gesichtsdetektion, die die Bildinformationen auf gesichtsähnliche Formen untersucht. Sofern ein Gesicht lokalisiert wurde, werden typischerweise im nächsten Schritt die Augen detektiert, da sie sich in der Regel aufgrund anderer Färbung vom restlichen Gesicht abheben. Abhängig vom eingesetzten Algorithmus werden weitere Gesichtsbereiche lokalisiert und anschließend das Gesicht normalisiert, um die Daten invariant gegenüber Drehung, Streckung und Stauchung zu speichern. Auf Basis dieser normalisierten Gesichter erfolgt dann die Merkmalsextraktion, die ebenfalls vom verwendeten Verfahren abhängig ist. Aus den Merkmalen werden im letzten Schritt mittels mathematischer Formulierungen Merkmalsvektoren generiert.

39 BSI, Gesichtserkennung, S.1, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf

40 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf

4.2
Infrarotkameras

Im Gegensatz zu Videokameras erfassen Infrarotkameras nicht das für das menschliche Auge sichtbare Licht, sondern elektromagnetische Strahlung im Infrarot-Bereich.

Nutzung zur Wärmebilderfassung

Bei der Wärmebilderfassung wird über die Intensität der Strahlung im Infrarotbereich auf die Temperatur eines Objekts geschlossen. Der Zusammenhang zwischen Strahlung und Temperatur wird mittels Boltzmann-Konstante hergestellt (Intensität der Strahlung = Boltzmann-Konstante * Temperatur). Das elektromagnetische Spektrum liegt bei Infrarotstrahlung zwischen 0.8 und 14 µm Wellenlänge, fällt also nicht in den für das menschliche Auge sichtbaren Bereich von 0.4 bis 0.7 µm.

Nutzung als Tiefenkameras (bspw.: Apple FaceID, Microsoft Kinect)

Tiefenkameras wurden ursprünglich zur Bewegungserkennung als natürliche Interaktion zwischen Mensch und Computer eingeführt.[41] Ein IR-Projektor sendet im nahen Infrarotbereich ein für das menschliche Auge nicht sichtbares codiertes Punktmuster aus. Ein CMOS-Sensor[42] empfängt das von der Szene reflektierte Bild und berechnet, aufgrund des Kameraabstandes über die Parallaxen korrespondierender Punkte, ein Tiefenbild. Punkte gleicher Größe wirken bei unterschiedlicher Entfernung unterschiedlich groß, bei bekannter Punktgröße kann auf die Entfernung zurückgeschlossen werden.

Nutzung zur Venenerkennung

Die Venenerkennung ist ein biometrisches Verfahren, mit dem Personen durch Infrarot-Technologie anhand ihrer Handgefäßstruktur erkannt werden können. Der Verlauf der Adern und Venen ist dabei genauso einzigartig wie der Fingerabdruck. Sensoren, die auf die Temperatur der Gefäßstruktur in der Hand reagieren, stellen in Kombination mit komplexer Filtertechnologie eine sogenannte Lebenderkennung fest und sollen somit vor Täuschungsversuchen mittels nichtbiometrischer Mittel oder durch Nachbildung biometrischer Merkmale schützen.

41 http://www.scanner.imagefact.de/de/depthcam.html

42 CMOS: complementary metal oxide semiconductor („komplementärer Metalloxid-Halbleiter“): eine bestimmte Form von Halbleiterbauelementen

4.3
Fingerabdruckleser

Der Prozess einer Fingerabdruckanalyse lässt sich in folgenden Schritten schematisch darstellen:[43]

– Aufnahme des Fingerabdruckbildes
– Bildqualitätsverbesserung
– Bildaufarbeitung
– Musterklassifizierung
– Merkmalsextraktion
– Verifikationsphase

Der grundlegende Aufbau eines optischen Fingerabdrucklesers besteht aus einer Lichtquelle, einem Glasprisma, einer Linse und einem Bildsensor. Der Finger wird auf das Glasprisma gedrückt, dabei haben Erhebungen direkten Kontakt mit dem Prisma, nur zwischen den Tälern und dem Prisma ist noch Luft. Das Licht wird von einer Seite ins Prisma gesendet. Es wird dann an den Tälern reflektiert und an den Erhebungen absorbiert bzw. zufällig gestreut. Die reflektierten Strahlen, die das Prisma verlassen, werden außerhalb durch die Linse auf einen Bildsensor gebündelt, in dem die Aufnahme stattfindet.

Bei jedem Sensor entsteht als Endprodukt im Allgemeinen ein Graustufenbild des Fingerabdruckes. Um ein Graustufenbild zu generieren gibt es zwei Modi: Beim *live scan* wird der Fingerabdruck durch einen Sensor aufgenommen, beim offline-Modus wird eine Aufnahme von hinterlassenen Fingerabdrücken, z. B. Gläsern, gemacht. Die Rohdaten werden mittels Bildverarbeitung verbessert und aufbereitet. Anschließend wird die Lage der Minuzien (Gabelung und Linienendung) in dem Fingerabdruck detektiert und extrahiert. In der Praxis weisen die aufgenommenen Fingerabdruckbilder eine unterschiedliche Qualität auf. Die Leistungsfähigkeit der Algorithmen kann durch mangelnde Bildqualität, verursacht durch Schmutz oder Verletzungen, beeinträchtigt werden.

Schließlich werden Entscheidungen, ob der ermittelte Merkmalsvektor einer vorhandenen Entität entspricht, auf Basis von Vergleichen zweier Merkmalsvektoren durchgeführt.

43 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/BiometrischeVerfahren/Fingerabdruckerkennung/fingerabdruckerkennung_node.html

4.4 Handgeometrieleser

Bei der Handerkennung sind relevante biometrische Merkmale die Höhe und Breite des Handrückens und der Finger sowie deren relative Lagen. Nicht relevant sind der Abdruck der Handflächen und die Fingerspitzen, da die Nägel nachwachsen und geschnitten werden.[44] Die Komponenten eines Handgeometrielesers sind meist in einem Gerät integriert. Dazu gehören eine CCD-Kamera zum Erfassen der Merkmale in Form einer 3D-Bildaufnahme, ein Display zur Interaktion mit dem Nutzer (Anzeige fehlerbehafteter Bereiche), ein Prozessor zum Erstellen und Überprüfen der Templates und ggf. Lesegeräte für ID-Karten oder PIN-Eingaben. Softwareseitige Komponenten sind vom jeweiligen Anwendungsfall abhängig.

Die Handerkennung erfordert eine korrekte Positionierung der Hand. Diese wird durch Orientierungshilfen erleichtert und durch visuelle Rückmeldung auf dem Display verdeutlicht.

Die Merkmalserfassung erfolgt durch eine CCD-Kamera, die mindestens zwei 3D-Bilder erstellt, je eines von oben und von der Seite. Definierte Charakteristika werden erfasst und in die Merkmale in Templates mit einer Größe von wenigen Byte gespeichert. Typischerweise werden nur um die 100 Charakteristika erfasst, was direkt eine geringe Einzigartigkeit zur Folge hat. Daher eignet sich dieses Verfahren weniger gut für die eindeutige Erkennung einer Person als z. B. Venenerkennung. Es kann allerdings zum Beispiel durch den Einsatz robuster Algorithmen „optimiert“ werden.[45]

4.5 Irisscanner

Der Prozess bei Irisscannern lässt sich schematisch folgendermaßen darstellen:[46]

– Bildaufnahme der Iris (Regenbogenhaut des Auges), meist im Nah-Infrarot-Bereich
– Iriserkennung

---

44 https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/07Hand_Retina/Handerkennung-Ausarbeitung.pdf

45 Singh, Hand geometry verification system: A review, S. 4, https://www.researchgate.net/profile/Amit_Singh202/publication/224086092_Hand_geometry_verification_system_A_review/links/5681052908ae1975838ead2f/Hand-geometry-verification-system-A-review.pdf?origin=publication_detail

46 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Iriserkennung_pdf.pdf

– Irissegmentierung
– Transformation des Kreissegments auf einen Streifen
– Binarisierung und Templateerstellung

Im Irisscanner wird die Iris durch eine Kamera erfasst und durch Bildverarbeitung isoliert, indem zwei Kreise (außen und innen) als Begrenzung der Iris dienen. Der resultierende Ring wird durch Polarkoordinaten repräsentiert, wodurch Invarianzen zur Irisgröße/-dicke ermöglicht werden. Daraufhin erfolgt eine spiralförmige Abtastung der Aufnahme und eine Gruppierung in helle und dunkle Bereiche (Binarisierung). Durch „Ausrollen" der Spirale kann eine Grafik, ähnlich eines Barcodes, generiert werden, die entsprechend mit den Templates verglichen wird.

Kommerzielle Erkennungsverfahren erfassen etwa 260 individuelle optische Merkmale der Iris. Diese Merkmale entwickeln sich aus einem zufallsgesteuerten, morphogenetischen Prozess in den ersten Lebensmonaten einer Person und bleiben über die restliche Lebenszeit weitgehend unverändert. Auch eineiige Zwillinge haben keine identische Iris-Struktur.[47]

4.6
Retinascanner

Der Prozess bei Retinascannern lässt sich folgendermaßen darstellen:

– Bildaufnahme der Retina (Netzhaut des Auges) durch kreisrunde Abtastung mit einem Laser
– Bildkorrektur bei Fehlsichtigkeiten der Linse
– Korrektur von Verdrehungen des Kopfes/der Retina
– Binarisierung und Templateerstellung

Der Retinascanner tastet die Retina mit einem Infrarot-Laser kreisrund ab. Eventuell vorhandene Fehlsichtigkeiten der Personen können und müssen bis zu gewissen Ausprägungen korrigiert werden, da ansonsten keine Normierung innerhalb der Template-Datenbank gegeben wäre. Das Phasen-Korrektur-Modul sorgt für die Bildkorrektur, falls der Kopf bzw. die Retina bei der Aufnahme verdreht erfasst wurde. Hierzu muss das digitale Abbild mehrfach in kleinen Schritten zum Referenzobjekt in der Datenbank verschoben und die Korrelation zwischen den jeweiligen Verschiebungen und der Referenz gebildet werden. Dadurch, dass Adern auf der Retina den Laserstrahl stärker absorbieren als umliegendes Gewebe, setzen sie sich kontrastreicher ab. Für die Binarisierung und Templateerstellung werden Schwellwerte definiert, so

47 https://de.wikipedia.org/wiki/Iris-Erkennung#Eigenschaften

dass sich die Bildinformationen der Blutbahnen von den restlichen Strukturen trennen lassen.

Je nach Hersteller erfolgt der Scan-Vorgang auf unterschiedlich definierte Weise, so dass es nicht direkt möglich ist, Systeme unterschiedlicher Hersteller miteinander zu vergleichen.

Weiterhin unterliegt die Retina degenerativen Veränderungen, so dass es im Laufe des Lebens zu unterschiedlichen Templates kommen kann. Die Retina eineiiger Zwillinge unterscheidet sich ebenfalls.

5.
Sammlung möglicher Einsatzszenarien („Use Cases“)

5.1
Übersicht über Einsatzszenarien

Es gibt zahlreiche Szenarien, bei denen biometrische Verfahren zum Einsatz kommen. Dies sind einerseits Szenarien, bei denen biometrische Erkennungssysteme mit dem unmittelbaren Ziel einer Identifikation oder Verifikation von Personen betrieben werden. Daneben gibt es Szenarien, bei denen Daten aus Verwendungszusammenhängen (etwa Videoüberwachung, Audiomitschnitte) mit Hilfe biometrischer Verfahren ausgewertet werden. Bei einigen dieser Verfahren ist ebenfalls eine Identifikation von Personen das Ziel; andere Verfahren zielen auf eine Wiedererkennung von Personen oder eine Gruppenzuordnung (Gefühlserkennung, Altersschätzung) ab. Szenarien sind u. a.:

– Identifikation
– Verifikation
– Wiedererkennung
– Profilbildung
– Gefühlsanalyse
– Beobachtung/Überwachung
– Registrierung
– Verhaltenssteuerung
– Werbung / Marketing
– Kommunikation
– Interaktion (Mensch – Maschine)

Die Einsatzszenarien aus Abschnitt 5.1 lassen sich unter verschiedenen Blickwinkeln gruppieren. Dazu gehören zum einen technische und funktionale Aspekte der biometrischen Verfahren, zum anderen die Zwecke, die mit dem Einsatz verfolgt werden.

5.2
Klassifikation der Szenarien nach technischen und funktionalen Aspekten

5.2.1
Kooperative biometrische Verifikation

Eine typische Funktion biometrischer Verfahren sind Authentisierungsverfahren (z. B. Zutrittskontrolle, Login, Entsperren), die kooperativ erfolgen: Die zu authentisierende Person verwendet das biometrische Verfahren bewusst mit dem Ziel, vom System erkannt zu werden (bewusste und kooperative Präsentation). Auch automatisierte Passkontrollen, bei denen die Übereinstimmung der in Ausweispapieren gespeicherten biometrischen Daten mit aktuell gewonnen Daten des Reisenden verglichen werden, fallen in diese Kategorie.[48] Gegebenenfalls sind mehrere Versuche bis zu einer positiven Authentisierung erforderlich. Zum Einsatz kommen Identifikations- und Verifikationsverfahren.

5.2.2
Nicht-kooperative biometrische Erkennung

Weitere typische Anwendungsfälle sind Überwachungsszenarien, bei denen eine Identitätsfeststellung (Identifizierung) oder Überprüfung einer Identität in einer Weise erfolgt, bei der die Person nicht kooperieren muss. Dies ist der Fall, wenn die biometrischen Charakteristika ohne bewusste Handlungen (kooperative Präsentation) der Person erfasst werden (können). Beispiele sind Video- oder Audioaufnahmen, die offen oder verdeckt erstellt werden oder die Auswertung anderweitig erfasster Daten (etwa Videoaufnahmen, Telefonate, Tastaturnutzungen) mit dem Ziel einer biometrischen Verarbeitung. Dies kann im Modus der bewussten oder indifferenten Präsentation erfolgten. Typische Szenarien sind hier Fahndungen oder Vergleiche mit biometrischen Referenz-Datenbanken im Sinne einer Identifikation.

In die Kategorie nicht-kooperativer Verfahren würde auch eine zwangsweise Nutzung biometrischer Verfahren aus dem Abschnitt 5.2.1 fallen.

48 Im Zusammenhang mit Grenzkontrollen sind weitere Nutzungen der aktuell gewonnen biometrischen Daten der Reisenden denkbar, etwa der Abgleich mit biometrischen Datenbanken (z. B. Fahndungsdatenbanken) im Hintergrund. Eine solche Nutzung ist dem Szenario 5.2.2 Nicht-kooperative biometrische Erkennung zuzuordnen.

5.2.3
Zuordnung zu Gruppen

Biometrische Verfahren werden nicht nur mit dem Ziel betrieben, einen eindeutigen Personenbezug herzustellen. Anwendungen können auch eine automatisierte Schätzung demographischer Daten (z. B. Alter, Geschlecht) oder die Zuordnung zu einer Gruppe (z. B. Altersgruppe, Brillenträger, Haar- und Augenfarbe, Zuordnung zu einer Ethnie etc.) vornehmen. Diese nicht personenindividuellen Merkmale werden auch als „soft biometrics" bezeichnet. Hierbei kommen in erster Linie Abbildungen von Gesichtern und der Iris zum Einsatz; denkbar sind auch Sprach- und Dialekterkennungen.

Die Zuordnung zu Gruppen mit Hilfe von „soft biometrics" kann auch verwendet werden, um die Anzahl der zu vergleichenden biometrischen Daten in Identifikationsverfahren zu reduzieren, wenn die zum Vergleich verwendeten biometrischen Daten ebenfalls klassifiziert sind (Beispiel: Geschlechtserkennung der aktuellen Person und Suche in Datenbanken nur bei Personen gleichen Geschlechts).

5.2.4
Profilbildung, Verkettung

Weiterhin können biometrische Verfahren mit dem Ziel betrieben werden, Handlungen einzelner Personen zu verketten. Ein typisches Beispiel ist die „Verfolgung" von Personen bei einer Videobeobachtung: Technisch liegen Videoaufzeichnungen als Datenstrom vor, der aus einzelnen Bildern (Frames) besteht. Die schnelle Abfolge beim Abspielen ergibt den Eindruck eines Films (wie beim Daumenkino). Sollen Personen gezählt oder eine Verweildauer ermittelt werden, so muss über mehrere Frames hinweg verglichen werden, ob es sich um dieselbe Person handelt oder nicht. Eine Identifizierung der Person ist nicht erforderlich.

5.2.5
Verhaltenserkennung

Verfahren können auch mit dem Ziel betrieben werden, Verhaltensweisen zu erkennen und die betroffenen Personen einer Verhaltensgruppe zuzuordnen. Beispielsweise lässt sich aus Gesichtsaufnahmen auf Gefühle (erregt, freundlich, ablehnend etc.)[49] schließen; ebenso aus Tonaufnahmen.

49 Siehe z. B. die „Emotion-API" der Firma Microsoft, https://azure.microsoft.com/de-de/services/cognitiveservices/emotion/?cdn=disable oder https://www.heise.de/newsticker/meldung/Software-erkennt-Gefuehle-2123851.html

5.3
Betrachtung der Szenarien nach Zwecken im datenschutzrechtlichen Sinn

5.3.1
Hoheitliche Authentisierungsverfahren

Typische Beispiele hoheitlicher Authentisierungsverfahren sind automatisierte Überprüfungen von biometrischen Daten (Gesichtsbild, Fingerabdruck) aus hoheitlichen Dokumenten (Reisepässe, Personalausweis, Aufenthaltstitel) mit den biometrischen Charakteristika des Ausweisinhabers.

5.3.2
Staatliche Identifikationsverfahren

Identifikationsverfahren kommen zum Einsatz, um einerseits unbekannte Personen erstmalig zu identifizieren (Identitätsfeststellung) oder um Doppelidentitäten zu entdecken. Ein Beispiel für den ersten Fall sind Abgleiche von Täterfotos (etwa auch Überwachungskameras von Geldautomaten) oder Videoaufzeichnungen mit Datenbanken, bei denen die biometrischen Daten mit identifizierenden Metadaten (z. B. einem Namen) verknüpft sind. Ein Beispiel für den zweiten Fall ist der Einsatz von Erkennungssystemen zur Aufdeckung von Doppelidentitäten, etwa bei Asylbewerbern.

5.3.3
Zutrittskontrolle

Das biometrische Verfahren wird zur Kontrolle eines physischen Zutritts zu Räumen oder Gebäuden verwendet. Typische verwendete biometrische Charakteristika sind Gesichtsform und Fingerabdrücke; andere Charakteristika wie Handgeometrie und Iris kommen auch zum Einsatz.

5.3.4
Zugangskontrolle

Das biometrische Verfahren wird zur Kontrolle des Zugangs zu Datenverarbeitungssystemen verwendet. Typische Szenarien sind die Entsperrung von Mobilgeräten mit Hilfe der biometrischen Charakteristika Gesichtsform und Fingerabdruck, aber auch Authentisierungsmechanismen (Log-in) auf Betriebssystemebene mit Hilfe von Gesichtsform und Fingerabdruck.

5.3.5
Werbung, Marketing

Werbe- und Marketingmaßnahmen können mit Hilfe biometrischer Verfahren auf bestimmte Gruppen, einzelne Personen oder auch deren Verhaltensweisen zugeschnitten werden.

Im ersten und dritten Fall werden die Zielpersonen Gruppen zugeordnet (z. B. Alter, Geschlecht, Bartträger, Brillenträger im ersten Fall, Gruppe der Ärgerlichen, Freundlichen oder Neutralen im dritten Fall) und entsprechende gruppenspezifische Werbemaßnahmen ausgewählt. Eine Identifizierung ist nicht erforderlich und wird auch meist nicht angestrebt; die Zuordnung zu einer Gruppe ist ausreichend. Wie bei der biometrischen Erkennung kann die Zuordnung zu einer Gruppe fehlerbehaftet sein.

Je nach Konstellation kann die Zuordnung zu einer Gruppe unter die Kategorie besonderer Daten fallen, wenn beispielsweise Gruppen nach sexuellen Präferenzen[50], Hautfarben oder körperlichen Einschränkungen gebildet werden.

Im zweiten Fall (Werbemaßnahmen für einzelne Personen) ist eine biometrische Erkennung erforderlich. Diese kann sich auf namentlich bekannte Personen (etwa VIPs, Stammkunden) und somit auf Personen mit bekannten Metadaten beziehen. Denkbar sind aber auch Fälle, bei denen lediglich eine Wiedererkennung („besucht zum dritten Mal in dieser Woche den Supermarkt“) erfolgt, ohne dass Metadaten zu einer Identifizierung verwendet werden.

5.3.6
Reichweitenmessung von Werbung

In einem weiteren Szenario wird mittels biometrischer Verfahren detektiert, durch welche Gruppen und wie lange Werbung betrachtet wird. Dazu werden während einer Werbemaßnahme die Betrachter erfasst und einer Gruppe zugeordnet (etwa Geschlecht oder Alter, siehe Abschnitt 5.3.5 Werbung, Marketing, 1. Fall) und die Betrachtungsdauer gemessen. Ebenso wird versucht, Reaktionen auf Werbemaßnahmen (Gefühlsregungen) zu erfassen. Hierbei kommen in erster Linie Verfahren zum Einsatz, die die biometrischen Charakteristika des Gesichts auswerten.

50 Siehe z. B. http://www.spiegel.de/netzwelt/netzpolitik/software-kann-homosexuelle-anhand-von-fotos-erkennen-a1166971.html

5.3.7
Beobachtung, Überwachung

In einem Überwachungsszenario werden biometrische Charakteristika (in erster Linie Gesichtsbilder und Sprache) erhoben (Video- und Audioaufnahmen) und mit bekannten biometrischen Daten, etwa aus einer Sperrliste (z. B. Personen mit Hausverbot) verglichen („Watchlist"). Dies kann mit hoheitlichen Anwendungen verknüpft werden (siehe Abschnitt 5.3.2).

5.3.8
Mensch-Maschine-Interaktion, Steuerung

Bei Interaktionen und Steuerungen von Maschinen können ebenfalls biometrische Verfahren zum Einsatz kommen. Beispiele reichen hier von einer reinen Anwesenheitserkennung über die Detektion von Aufmerksamkeit und Position von Personen in Kraftfahrzeugen (teilautonomes Fahren), einer Einschätzung aktueller Verhaltensweisen (defensive/sportliche Fahrweise) bis zu einer Personenerkennung des Fahrers mit dem Ziel einer individuellen Konfiguration des Fahrzeugs (Sitz- und Spiegelposition, Radiosender).

In einen ähnlichen Anwendungsbereich fällt eine Gruppenzuordnung von Personen aus dem Umfeld des Kfz (etwa zur Unterscheidung von Altersgruppen von Passanten mit dem Ziel, beim Erkennen von Kindern bremsbereit zu sein).

Andere Steuerungsmechanismen basieren auf einer Sprechererkennung, etwa im Bereich der Heimautomatisierung.

Nicht alle dieser Anwendungen erfordern die Identifikation von Personen. So kann mit biometrischen Verfahren ermittelt werden, ob Fahrerinnen und Fahrer hinreichend konzentriert sind.

6.
Rechtliche Bewertung

Nach Art. 9 Abs. 1 DS-GVO ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person grundsätzlich untersagt. In den in Art. 9 Abs. 2 DS-GVO normierten Fällen ist sie ausnahmsweise erlaubt. Erfolgt die Verarbeitung biometrischer Daten nicht zur eindeutigen Identifizierung einer natürlichen Person, sondern zu einem anderen Zweck, richtet sich ihre Zulässigkeit nach Art. 6 Abs. 1 DS-GVO. In jedem Fall ist die Eignung biometrischer Daten zur eindeutigen Identifizierung im Wege biometrischer Analyseverfahren bei der Risikoabschätzung und der Auswahl der technischen und organisatorischen Maßnahmen zu berücksichtigen.

6.1
Begriff der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO

Biometrische Daten sind nach der Definition in Art. 4 Nr. 14 DS-GVO mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

6.1.1
Personenbezogene Daten

Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Im Prinzip ist jedes eindeutige biometrische Merkmal ein individuelles Personenkennzeichen[51] und daher ein personenbezogenes Datum.

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten nach Erwägungsgrund 26 alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. Durch den ausdrücklichen Bezug auf die technologische Entwicklung dynamisiert die DS-GVO den Begriff der Identifizierbarkeit und verpflichtet Verantwortliche, Aufsichtsbehörden und Gerichte, in Zukunft dieser Entwicklung zu folgen und gegebenenfalls die Identifizierbarkeit von Datenbeständen neu zu bewerten. Um den Zweck des Schutzes der betroffenen Personen vor Beeinträchtigung ihrer Grundrechte durch die Verarbeitung von Daten

51 Weichert, Biometrie – Freund oder Feind des Datenschutzes? in: CR 1997, S. 369.

zu erreichen, müssen die tatsächlich verfügbaren und nicht nur die rechtlich zulässigen Möglichkeiten berücksichtigt werden.[52]

Die Grundsätze des Datenschutzes sollten nach Erwägungsgrund 26 nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Nichts am Personenbezug der verarbeiteten Daten ändert hingegen deren Pseudonymisierung. Gemäß Art. 4 Nr. 5 DS-GVO ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Da der Verantwortliche weiterhin in der Lage ist, die betroffenen Personen zu identifizieren, bleibt der Personenbezug pseudonymisierter Daten erhalten. Das ergibt sich auch aus Erwägungsgrund 26.

Nach Ansicht der früheren Artikel-29-Datenschutzgruppe[53] gilt ein Referenz-Template, das von dem Bild einer Person geschaffen wurde, als personenbezogenes Datum, da es einen Satz unverwechselbarer Merkmale des Gesichts einer Person enthält, der dann mit einer bestimmten Person verlinkt wird und als Referenz für spätere Vergleiche zur Identifizierung und Verifizierung gespeichert wird.

6.1.2
Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person

Mit biometrischen Daten im Sinne der DS-GVO werden Seins-Merkmale wie körperliche Eigenschaften oder Verhaltensweisen angesprochen, die unmittelbar einer Person zugeordnet werden können und in der Regel dauerhaft an eine Person gebunden sind. Eine (beabsichtigte oder unfreiwillige) Trennung

52 Klabunde, in: Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 13

53 Die Artikel-29-Datenschutzgruppe war ein unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Mit dem Inkrafttreten der Datenschutzgrundverordnung wurde die Artikel-29-Datenschutzgruppe durch den Europäischen Datenschutzausschuss (EDSA) abgelöst. Der EDSA hat sich dazu noch nicht geäußert.

von der Person kann grundsätzlich nicht stattfinden.[54] Die biologischen oder verhaltensabhängigen Charakteristika eines Individuums, von welchem sich zur Unterscheidung verwendbare, reproduzierbare biometrische Merkmale ableiten lassen, die zum Zweck der automatisierten biometrischen Erkennung einsetzbar sind, nennt man „biometrische Charakteristika". Sie sind der Ausgangspunkt für alle biometrischen Erkennungssysteme.

6.1.3
Daten, die die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen

Biometrische Daten sind zur eindeutigen Identifizierung einer natürlichen Person geeignet, wenn die gemessenen Merkmale einzigartig sind. Nicht notwendig ist, dass die Angaben weltweit eindeutig sind. Es genügt, dass eine genaue Identifizierung in einer mit abstrakten Merkmalen beschriebenen Gruppe einer großen unbestimmten Zahl von Personen möglich ist. Relevant ist, dass die über die natürliche Person erfassten Daten objektiv unverwechselbar sind. Wegen ihrer Verbindung mit dem menschlichen Körper sind sie nicht oder nur schwer zu verändern oder zu verfälschen. Dessen ungeachtet können sich z. B. auf Grund des Alters oder von Krankheiten Veränderungen ergeben, die eine Zuordnung erschweren oder gar unmöglich machen. Auch das Fehlen von bestimmten biometrischen Merkmalen (etwa von Fingerabdrücken) bei einer bestimmten Person kann zu deren Identifizierung geeignet sein.[55]

6.1.4
Mit speziellen technischen Verfahren gewonnene Daten

Die Definition nimmt Bezug auf „spezielle technische Verfahren". In der englischen Fassung wird hier der Begriff „specific technical processing" benutzt, also „bestimmte technische Verfahren".[56] Dabei kann es sich nur um solche Verfahren handeln, die Daten liefern, die nach dem Stand der Technik die eindeutige Identifizierung einer natürlichen Person mit einem biometrischen Erkennungssystem ermöglichen.

Hierzu ist es erforderlich, dass der Informationsgehalt der Daten für eine eindeutige Identifizierung ausreicht. Biometrische Daten sind daher sowohl

54 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/ einfuehrung.html

55 Weichert, in Kühling/Buchner, DS-GVO, Art. 4 Nr. 14, Rn. 2.

56 Im Folgenden wird daher dieses Begriffsverständnis zugrunde gelegt.

die biometrischen Samples, also die direkt mit einem Sensor erfassten Merkmale, wie auch die sogenannten Templates, das heißt die aus biometrischen Samples gewonnenen und typisierten Merkmals-Vektoren, die auf der Grundlage eines mathematischen Modells standardisiert erfasst und regelmäßig zur Grundlage für digitale Zuordnungen genommen werden.[57]

6.1.5
Verhältnis zum Begriff der biometrischen Daten nach ISO/IEC JTC SC37

Nach dem durch ISO/IEC JTC SC37 international standardisierten biometrischen Vokabular sind biometrische Daten biometrische Samples oder Ansammlungen biometrischer Samples in jeder Verarbeitungsstufe, biometrische Referenzen, biometrische Proben, biometrische Merkmale oder biometrische Eigenschaften. Demgegenüber sind biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen. Sowohl die DS-GVO als auch das international standardisierte Vokabular haben jedoch die Verarbeitung biometrischer Verfahren zum Zweck der eindeutigen Identifizierung im Fokus.

Der Begriff der biometrischen Daten aus dem international standardisierten biometrischen Vokabular kann daher zur näheren Bestimmung des Begriffs der biometrischen Daten nach Art. 4 Nr. 14 DS-GVO herangezogen werden. Allerdings zählen nach dem biometrischen Standard-Vokabular auch solche biometrischen Eigenschaften zu den biometrischen Daten, die nicht für sich genommen die eindeutige Identifikation einer natürlichen Person ermöglichen. Daten wie Alter, Größe und Geschlecht, bei denen es sich zwar um biometrische Daten im Sinne des biometrischen Standardvokabulars handelt, dürften grundsätzlich nicht allein die eindeutige Identifizierung einer natürlichen Person im Sinne der DS-GVO ermöglichen. Je nach Einzelfall kann es hiervon Ausnahmen geben. So genügt zur eindeutigen Identifizierung einer natürlichen Person die Angabe des Geschlechts, wenn es in einer Gruppe von Menschen nur eine Person dieses Geschlechts gibt.

Als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO können danach sowohl die biometrischen Samples, also die analogen oder digitalen Repräsentationen biometrischer Charakteristika vor der biometrischen Merkmalsextraktion, als auch die biometrischen Merkmale, das heißt die Zahlen oder

57 Weichert, a. a. O., Rn. 7.

markanten Kennzeichen, die aus einem biometrischen Sample extrahiert wurden und zum Vergleich verwendet werden können, eingestuft werden.

Klarere Konturen erhält der Begriff der biometrischen Daten ferner dadurch, dass das international standardisierte biometrische Vokabular die biometrische Erkennung als automatisierte Erkennung beschreibt, also als die Erkennung mittels eines rechnergestützten Systems. Das bedeutet, dass von biometrischen Daten erst dann die Rede sein kann, wenn diese für eine automatisierte Verarbeitung geeignet sind. Dieses Begriffsverständnis passt zu dem der DS-GVO: Danach sind biometrische Daten mit speziellen technischen Verfahren gewonnene Daten. Dies setzt ein zumindest teilweise automatisiertes Verfahren zur Gewinnung voraus. Zudem ist eine automatisierte Verarbeitung biometrischer Daten mittels biometrischer Erkennungsverfahren zum Zwecke der eindeutigen Identifizierung für die betroffenen Personen mit erhöhten Risiken verbunden. Die so verarbeiteten Daten sind deshalb nach Art. 9 Abs. 1 DS-GVO als besondere Kategorie personenbezogener Daten einzustufen, deren Verarbeitung nach Art. 9 Abs. 2 DS-GVO einer besonderen Rechtfertigung bedarf.

6.1.6
Beispiele für biometrische Daten gemäß Art. 4 Nr. 14 DS-GVO

6.1.6.1
Fingerabdrücke

Eine Aufnahme der Papillarleisten an der Fingerkuppe ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person.

Sie lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einer solchen Aufnahme handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.2
Aufnahmen der Irisstrukturen

Eine Aufnahme der Irisstrukturen ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Sie lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einer solchen Aufnahme handelt es sich um ein biometri-

sches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.3
Retinascans

Ein Retinascan ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Er lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Retinascan handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.4
Handvenenbilder

Ein Bild des Handvenenmusters ist ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen einer Person. Es lässt sich einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Bild des Handvenenmusters handelt es sich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.5
Handgeometrie

Aufnahmen der Handgeometrie sind mit einem speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physiologischen Merkmalen einer Person. Sie lassen sich einer natürlichen Person eindeutig zuordnen und ermöglichen dadurch die eindeutige Identifizierung einer natürlichen Person. Bei den Aufnahmen handelt es sich um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO.

6.1.6.6
Gesichtsbilder

Ein Gesichtsbild ist dann ein mit einem speziellen technischen Verfahren gewonnenes personenbezogenes Datum zu den physiologischen Merkmalen

einer Person, wenn dieses die Verarbeitung biometrischer Charakteristika des Gesichts zur Erstellung eines biometrischen Templates oder strukturierter Sammlungen von Gesichtsbildern ermöglicht. Das Gesichtsbild lässt sich dann im Rahmen eines automatisierten Verfahrens einer natürlichen Person eindeutig zuordnen und ermöglicht dadurch die eindeutige Identifizierung einer natürlichen Person. Bei einem Gesichtsbild handelt es sich unter den vorgenannten Voraussetzungen um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO und zugleich auch um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO.

Im Gegensatz zu Gesichtsbildern (wie in Art. 4 Nr. 14 DS-GVO als biometrisches Datum genannt) sind Lichtbilder oder Videoaufnahmen von Personen nicht per se biometrische Daten gem. Art. 4 Nr. 14 DS-GVO.

Auf Lichtbildern oder Videoaufnahmen können aber biometrische Daten enthalten sein, wenn das Gesicht einer Person in entsprechender Auflösung, Ausrichtung und Größe auf dem Lichtbild oder der Videoaufnahme abgebildet wird.

6.2
Voraussetzungen des Art. 9 DS-GVO

6.2.1
Grundsätze

Die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person ist gemäß Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt. Eine Verarbeitung im Sinne des Art. 9 Abs. 1 DS-GVO liegt vor, wenn die eindeutige Identifizierung einer natürlichen Person im Vordergrund steht. Die englische Fassung wird noch deutlicher, da hier von „the purpose of uniquely identifying a natural person“ die Rede ist. Dies macht klarer als das deutsche „um … zu“, dass hier der Zweck (purpose) einer eindeutigen Identifizierung hinter der Verarbeitung stehen muss.

Identifizierung im Sinne der Verordnung umfasst nicht jedwede Erkennungsmöglichkeit im Zusammenhang mit biometrischen Daten. Zielrichtung des Art. 9 DS-GVO ist es, die Verarbeitung von besonders sensiblen personenbezogenen Daten einzuschränken und nur unter besonderen Voraussetzungen zuzulassen. Biometrische Daten zählen aufgrund ihrer Vielfältigkeit nur dann zu diesen Daten, im Gegensatz zu den übrigen in Art. 9 DS-GVO erwähnten, wenn sie mit besonderer Zweckbestimmung, nämlich zur eindeutigen Identifizierung und damit in besonders risikobehafteter Weise verarbeitet werden. Dieses erhöhte Risiko besteht nur dann, wenn automatisierte biometrische Erkennungsverfahren eingesetzt werden. Der in Art. 9 Abs. 1 DS-GVO

verwendete Begriff der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person entspricht dem der biometrischen Erkennung im international standardisierten biometrischen Vokabular.

Von einer biometrischen Erkennung kann nur bei einer automatisierten Erkennung die Rede sein, also bei einer Erkennung mittels eines rechnergestützten Systems. Eine manuelle Sichtkontrolle fiele nach diesem Verständnis aus dem in Art. 9 Abs. 1 DS-GVO verwendeten Begriff der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person heraus.

Die biometrische Erkennung umfasst biometrische Verifikation und biometrische Identifikation. Die biometrische Verifikation meint nach dem international standardisierten biometrischen Vokabular den Prozess, in dem eine biometrische Behauptung durch einen biometrischen Vergleich bestätigt wird. Der Begriff der biometrischen Behauptung bezeichnet die Behauptung, dass eine zu erfassende betroffene Person die körperliche Quelle einer bestimmten biometrischen Referenz ist. Biometrische Referenz nennt man ein oder mehrere gespeicherte biometrische Samples, biometrische Templates oder biometrische Modelle, die einer betroffenen Person zugeordnet wurden und als Objekt zum biometrischen Vergleich verwendet werden. Die biometrische Referenz kann sich in einer Datenbank, verteilt in einem Netzwerk oder auf einer Smartcard befinden.

Als biometrische Identifikation wird der Prozess der Suche in einer biometrischen Enrolmentdatenbank nach dem Identifikator einer biometrischen Referenz, der einem einzigen Individuum zugeordnet werden kann, bezeichnet. Eine biometrische Enrolmentdatenbank besteht aus Datensätzen enrolter Personen, die nicht-biometrische Daten sowie Identifikatoren biometrischer Referenzen beinhalten. Als Identifikator einer biometrischen Referenz bezeichnet man den Zeiger auf einen biometrischen Referenzdatensatz in der biometrischen Referenzdatenbank. Ein Referenzdatensatz ist ein indexierter Datensatz, der biometrische Referenzen beinhaltet. Hierbei ist zu beachten, dass eine einzelne biometrische Referenz (z. B. ein auf einer Speicherkarte gespeicherter Fingerabdruck) in einigen Transaktionen als biometrische Enrolmentdatenbank betrachtet werden kann.

Während der Anwender bei der Verifikation dem biometrischen System seine Identität vorab bekannt gibt (z. B. die User-ID über Tastatur oder Karte) und das System das biometrische Merkmal dann nur noch mit dem einen zur User-ID passenden Referenzmerkmal vergleichen muss (1:1-Vergleich), wird

bei der Identifikation das biometrische Merkmal mit allen im biometrischen System gespeicherten Referenzmerkmalen verglichen (1:n-Vergleich).[58]

Auch Erwägungsgrund 51 legt nahe, dass die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung gemäß Art. 9 Abs. 1 DS-GVO sowohl Verfahren zur Identifikation als auch zur Authentisierung umfasst. Die Verfahren unterscheiden sich nur in der Anzahl der zum Vergleich herangezogenen Referenzdatensätze: Bei der Authentisierung wird gegen genau einen Referenzdatensatz geprüft, bei der Identifikation gegen mehrere. Dem so gebrauchten Begriff der Authentisierung entspricht im biometrischen Standardvokabular der Begriff der biometrischen Verifikation.

Biometrische Daten fallen somit erst unter den Begriff der „besonderen Kategorien personenbezogener Daten“ gemäß Art. 9 Abs. 1 DS-GVO, wenn sie zur eindeutigen Identifizierung einer natürlichen Person, das heißt zum Zweck der automatisierten biometrischen Erkennung verarbeitet werden. In diesem Fall ist der Anwendungsbereich der oben genannten Regelung eröffnet.

6.2.2
Ausgewählte Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO

Nicht untersagt ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person in den Fällen des Art. 9 Abs. 2 DS-GVO.

6.2.2.1
Art. 9 Abs. 2 lit. a DS-GVO

Die betroffene Person hat in die Verarbeitung ihrer biometrischen Daten zur Identifizierung ausdrücklich eingewilligt. Die Einwilligung muss sich dabei explizit auf die Verwendung der biometrischen Daten beziehen. Es muss somit eine ausdrückliche Bezugnahme auf die Daten in der Einwilligung vorliegen. Dies setzt voraus, dass auf die Sensitivität der Daten gesondert hingewiesen wird.[59] Durch die DS-GVO werden sämtliche personenbezogenen Daten geschützt, die in Art. 9 Abs. 1 DS-GVO genannten jedoch in besonderer Weise. Durch die Hinweise soll der Betroffene in die Lage versetzt werden zu entscheiden, ob er sich möglicherweise mit der Einwilligung in

58 BSI, Einführung in die technischen Grundlagen der biometrischen Authentisierung, S. 1, erhältlich unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Technische_Grundlagen_pdf.pdf

59 Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 47

die Datenverarbeitung außerhalb dieses besonderen rechtlichen Schutzes befindet. Eine konkludente Einwilligung ist somit nicht möglich.

Es ist der konkrete Zweck der Datenverarbeitung zu nennen. Dies wäre gemäß Art. 9 Abs. 1 DS-GVO zumindest der Zweck der eindeutigen Identifizierung.

An das Erfordernis einer freiwilligen Einwilligung in die Verarbeitung biometrischer Daten sind besonders hohe Anforderungen zu stellen, wenn sie im Rahmen eines Abhängigkeitsverhältnisses, wie zum Beispiel im Beschäftigtenverhältnis, erteilt wird.

6.2.2.2
Art. 9 Abs. 2 lit. b DS-GVO

Die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann. Art. 9 Abs. 2 lit. b DS-GVO ist kein aus sich heraus anwendbarer eigenständiger Erlaubnistatbestand, sondern verlangt vielmehr, dass sich die Erforderlichkeit der Datenverarbeitung zu vorgenannten Zwecken aus einer gesonderten, konkreten unionsrechtlichen oder einzelstaatlichen Norm, wozu auch Betriebsvereinbarungen und Tarifverträge zählen, ergibt.[60]

Biometrische Daten können im betrieblichen Kontext bei der Zugangsberechtigung, der Authentisierung an IT-Systemen oder bei der Einlasskontrolle zu besonders schützenswerten Bereichen zum Einsatz kommen. Das Erforderlichkeitsprinzip ist in diesem Bereich eng auszulegen.[61]

6.2.2.3
Art. 9 Abs. 2 lit. e DS-GVO

Eine Verarbeitung sensibler Daten kann nach Art. 9 Abs. 2 lit. e DS-GVO ferner dann erlaubt sein, wenn die betroffene Person die Daten offensichtlich öffentlich gemacht hat. Unter Öffentlichkeit in diesem Sinne ist die Allgemeinheit, also ein individuell nicht bestimmbarer Personenkreis zu verstehen. Außerdem muss die „betroffene Person“ die sensiblen Daten „offensichtlich“ öffentlich gemacht haben. Dies setzt einen unzweideutigen, bewussten Willensakt voraus, der final auf die Entäußerung des Datums in die Öffentlichkeit in dem erläuterten Sinne gerichtet ist. Durch dieses Merkmal soll verhindert

60 Schulz, in: Gola, DS-GVO, Art. 9 Rn. 18

61 Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 54

werden, dass ein Betroffener dadurch den besonderen Schutz verliert, dass ein Dritter dessen sensitive Daten in die Öffentlichkeit trägt, oder dass dies durch den Betroffenen selbst unbeabsichtigt geschieht.[62]

Das bloße „Dasein" im öffentlichen Raum fällt nicht unter den Begriff der Veröffentlichung in diesem Sinne. Denn der entäußernde Charakter eines Willensaktes, bestimmte Daten einem unbestimmten Personenkreis zugänglich zu machen, kann nicht mit dem Bewegen im öffentlichen Raum gleichgesetzt werden. Damit ist insbesondere ausgeschlossen, dass Bildaufnahmen von Personen im öffentlichen Raum getätigt werden, um diese mittels eines Gesichtserkennungsprogramms zu verarbeiten oder um Personen auf politischen Veranstaltungen im öffentlichen Raum zu registrieren.[63]

6.2.2.4
Art. 9 Abs. 2 lit. f DS-GVO

Zulässig ist die Verarbeitung gemäß Art. 9 Abs. 2 lit. f DS-GVO auch dann, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Ansprüche im Sinne des lit. f müssen nicht rechtshängig sein, so dass auch der vor- und außergerichtliche Rechtsverkehr erfasst wird.[64]

6.2.2.5
Art. 9 Abs. 2 lit. g DS-GVO

Die Verarbeitung ist gemäß Art. 9 Abs. 2 lit. g DS-GVO auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats aus Gründen eines erheblichen öffentlichen Interesses erforderlich. Es handelt sich hier nicht um einen eigenen Erlaubnistatbestand, sondern um eine Öffnungsklausel. Es werden besonders schützenswerte Belange des Gemeinwohls bzw. der Gemeinschaftsgüter erfasst. Das Gemeinwohlinteresse muss das Persönlichkeitsrecht der betroffenen Person überwiegen.

6.3
Anwendung des Art. 6 Abs. 1 DS-GVO

Zusätzlich zu den speziellen Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten sollen nach Erwägungsgrund 51 die

62 Weichert in Kühling/Buchner, DS-GVO, Art. 9 Rn. 79

63 Schiff, in: Ehmann/Selmayr, DS-GVO, Art. 4 Rn. 40, 41

64 Schulz, in: Gola, DS-GVO, Art. 9 Rn. 27

allgemeinen Grundsätze und andere Bestimmungen der DS-GVO, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Bei besonders schutzbedürftigen Daten ist die Eingriffsintensität regelmäßig höher, weshalb höhere Anforderungen an die Rechtfertigung des Eingriffs zu stellen sind. Dies hat zur Folge, dass Art. 9 DS-GVO den Art. 6 DS-GVO nicht verdrängt, sondern dass seine Voraussetzungen zusätzlich zu denen des Art. 6 DS-GVO vorliegen müssen.

Werden zudem biometrische Daten nicht zur eindeutigen Identifizierung einer natürlichen Person, sondern zu anderen Zwecken verarbeitet, ist Art. 6 Abs. 1 DS-GVO einschlägig. Danach ist die Verarbeitung von personenbezogenen Daten nur rechtmäßig, wenn mindestens eine der darin geregelten Bedingungen erfüllt ist.

6.3.1
Einwilligung in die Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. a DS-GVO rechtmäßig, wenn die betroffene Person ihre Einwilligung erteilt hat. Eine Einwilligung ist nur unter den Voraussetzungen der hinreichenden Information und Freiwilligkeit möglich. Besondere Konstellationen wie beispielsweise eine Einwilligung im arbeitsrechtlichen Kontext sind auch hier zu berücksichtigen.

6.3.2
Erforderlichkeit zur Erfüllung eines Vertrages oder eines vorvertraglichen Verhältnisses gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. b DS-GVO rechtmäßig, wenn sie für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Neben der „Erfüllung“ sind die Vorbereitung und Anbahnung des Vertrages, dessen Durchführung sowie auch dessen Abwicklung insbesondere zur Erfüllung von Gewährleistungspflichten oder sekundären Leistungspflichten erfasst. Auch vorvertragliche Maßnahmen können eine Verarbeitung legitimieren, allerdings nur, wenn sie „auf Anfrage der betroffenen Person erfolgen“.[65]

Für die Erfüllung eines Vertrags ist eine Verarbeitung nur dann erforderlich, wenn sie für die Vertragszwecke notwendig ist. Das ist etwa der Fall bei der Speicherung einer Iris-Abbildung zur Herstellung eines Deko-Objektes aus dieser Abbildung, der Mitteilung von Kreditkartendetails zur Abwicklung der Zahlung eines Online-Kaufs, der Anschrift des Kunden für die vertraglich

65 Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 6 DSGVO, Rn.10

bedingte Korrespondenz oder bei der Angabe der Bankverbindung für die Gehaltsüberweisung. Dagegen ist die Speicherung von Kundenpräferenzen für Marketingzwecke nicht für die Erfüllung des Vertrags erforderlich.[66]

6.3.3
Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO

Die Verarbeitung ist gemäß Art. 6 Abs. 1 S. 1 lit. f DS-GVO rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Die Datenverarbeitung muss im berechtigten Interesse des Verantwortlichen oder eines Dritten liegen. Das berechtigte Interesse kann rechtlicher, wirtschaftlicher oder ideeller Natur sein. In EG 47 sind Beispiele für das berechtigte Interesse aufgeführt. Dies sind die Verhinderung von Betrug und Zwecke der Direktwerbung. Zu bestimmen ist als erstes das Interesse der verantwortlichen Stelle auf Grundlage der Zweckbestimmung.

Die Verarbeitung muss ferner zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein.

Den berechtigten Interessen der Verantwortlichen Stelle dürfen keine überwiegenden Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person entgegenstehen.

Dabei sind die für beide Seiten bestimmten Interessen zu gewichten. Die zum bislang geltenden Recht entwickelten Faktoren der Gewichtung behalten dabei auch in Ansehung der DS-GVO ihre Gültigkeit, wobei künftig dem Ausfluss europäischer Grundfreiheiten und -rechte besondere Bedeutung zukommt.[67]

Als Abwägungskriterium kommt noch die vernünftige Erwartungshaltung der betroffenen Person hinzu (EG 47). Im Rahmen der Interessenabwägung ist somit zu berücksichtigen, ob eine betroffene Person zum Zeitpunkt der Datenerhebung und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffen Person vernünftigerweise nicht mit der weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Personen überwiegen.[68]

---

66 Heberlein, in: Ehmann/Selmayr, Art. 6 DS-GVO, Rn. 13

67 Schulz, in: Gola, DS-GVO, Art. 6 Rn. 53

68 Schulz in Gola, DS-GVO § 6 Rn. 55

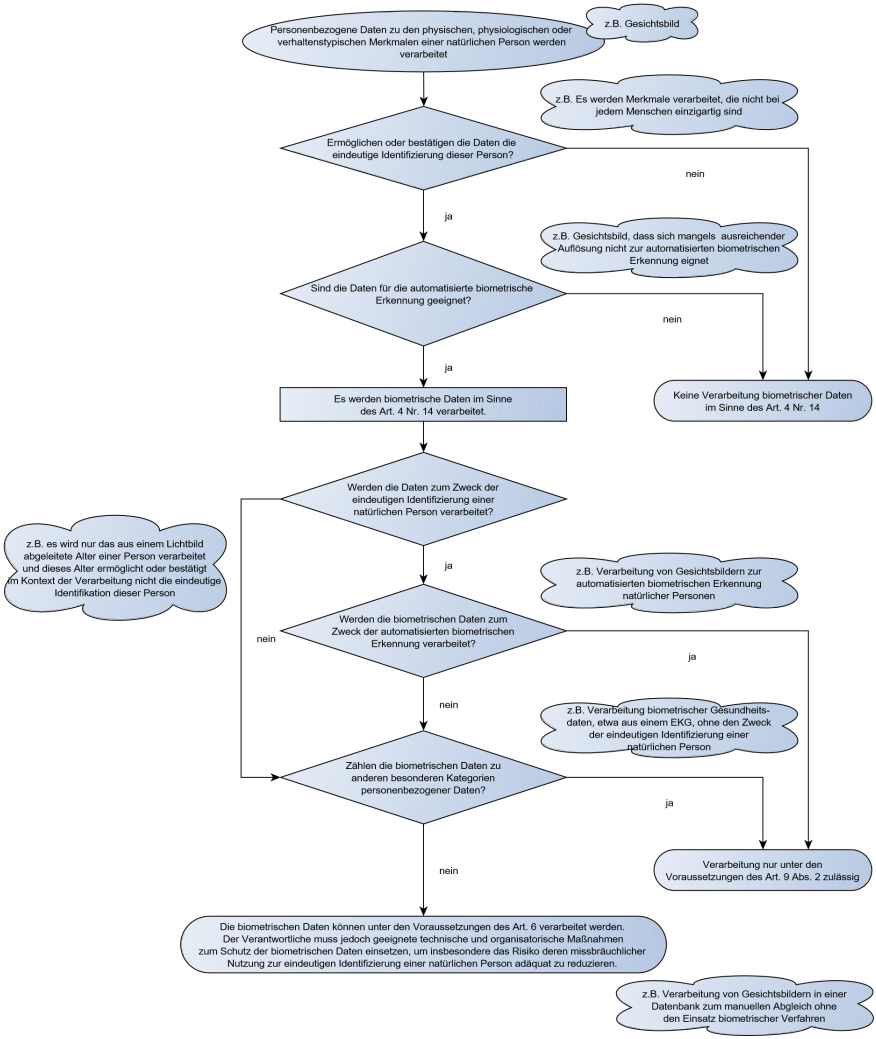

Abbildung 1 – Flussdiagram zur Klassifizierung von Verarbeitungen von Daten zu physischen, physiologischen oder verhaltenstypischen Merkmalen natürlicher Personen

6.4
Juristische Bewertung anhand ausgewählter Anwendungsfälle

6.4.1
Fall 1: Bezahlung des Schulessens mit Hilfe des Fingerabdrucks

Ein Unternehmen, das von einem Caterer zum Zwecke der Abrechnung der Mittagessen hinzugezogen wurde, bietet mehrere Methoden an, mit denen sich die Schulkinder bei der Mittagessensausgabe identifizieren können. Zu diesen Methoden gehört unter anderem die Identifikation mittels biometrischer Daten. Dabei wird der Fingerabdruck elektronisch eingelesen, gespeichert und zu Identifikationszwecken genutzt; das dabei erzeugte Template wird zur Identifikation innerhalb der jeweiligen Schülerschaft eingesetzt. Will sich ein Kind bei der Mittagessensausgabe identifizieren, so legt es seinen Finger auf, dabei wird erneut ein Template errechnet und mit den gespeicherten Templates verglichen. Liegt eine Übereinstimmung vor, so ist das Kind identifiziert, erhält das gebuchte Essen und die finanzielle Abrechnung kann digital erfolgen.

Bei den verarbeiteten elektronischen Fingerabdrücken der Schüler handelt es sich um daktyloskopische und damit um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Diese werden auch im Sinne des Art. 9 Abs. 1 DS-GVO zum Zweck der eindeutigen Identifizierung der Schüler verarbeitet, da die ausgegebenen Essen zu Abrechnungszwecken bestimmten Schülern zugeordnet werden sollen. Als einzige Rechtsgrundlage für diese Verarbeitung kommt eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht.

Die Einwilligung muss wirksam sein. Zu den Elementen einer wirksamen Einwilligung gehören Freiwilligkeit und Informiertheit. Solange ein Caterer mehrere gleichwertige und nicht-diskriminierende Methoden anbietet, mit deren Hilfe sich die Schüler bei der Essensausgabe identifizieren können, kann eine von den Eltern oder den einwilligungsfähigen Schülern erteilte Einwilligung in die Verarbeitung biometrischer Daten als „freiwillig“ angesehen werden. Angesichts der besonderen Schutzbedürftigkeit dieser Daten sind an die Freiwilligkeit – auch bei der angebotenen Alternative – strenge Maßstäbe anzulegen. Es muss sich um eine echte – und nicht nur formale – Alternative handeln, die z. B. nur in den AGB steht.

Auch an die Informiertheit müssen bei biometrischen Verfahren hohe Anforderungen gestellt werden. Da biometrische Daten als individuelle und universale Identifikatoren dienen können, ist die Bereitstellung klarer und leicht zugänglicher Informationen über die Nutzung der jeweiligen Daten als unabdingbare Voraussetzung für eine faire Verarbeitung zu betrachten. Wenn insbesondere der eingesetzte Algorithmus dasselbe biometrische

Template auch in anderen biometrischen Systemen erzeugt, muss die betroffene Person wissen, dass sie auch in anderen biometrischen Systemen wiedererkannt werden kann.[69]

6.4.2
Fall 2: Zugang zu Firmenräumen mit Hilfe des Fingerabdrucks

Eine Firma, die im Internet mit Holzfenstern handelt und ungefähr 50 Mitarbeiter hat, plant den Einsatz eines biometrischen Zugangssystems mittels Fingerabdruck. Die Firma hat kein sicherheitsrelevantes Tätigkeitsgebiet; es besteht kein Unterschied zu anderen, „normalen" Firmen. Der beabsichtigte Zweck (Zugangskontrolle) könnte auch mit einer Chipkarte, einem PIN-Code oder einem Passwort sichergestellt werden.

Bei den verarbeiteten elektronischen Fingerabdrücken der Mitarbeiter handelt es sich um daktyloskopische und damit um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Diese werden auch im Sinne des Art. 9 Abs. 1 DS-GVO zur eindeutigen Identifizierung der Mitarbeiter verarbeitet, da nur sie Zugang zu den Firmenräumen erhalten sollen. Als einzige Rechtsgrundlage für diese Verarbeitung kommt eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO in Betracht.

Um wirksam zu sein, muss die Einwilligung insbesondere freiwillig erfolgt sein. Nach Maßgabe des Erwägungsgrundes 43 ist eine Einwilligung dann nicht als freiwillig anzusehen, wenn ein klares Ungleichgewicht zwischen betroffener Person und dem Verantwortlichen der Datenverarbeitung besteht. Dies ist grundsätzlich im Rahmen von Arbeitsverhältnissen anzunehmen. Dennoch sind nach Ansicht des Europäischen Datenschutzausschusses auch im Rahmen von Arbeitsverhältnissen Situationen denkbar, in denen ein Arbeitgeber nachweisen kann, dass die Einwilligung in eine Verarbeitung freiwillig erfolgte, insbesondere dann, wenn die Verweigerung der Einwilligung keinerlei nachteilige Folgen für den Arbeitnehmer gehabt hätte.[70]

Auch nach § 26 Abs. 2 BDSG kann eine Verarbeitung personenbezogener Daten von Beschäftigten grundsätzlich auf der Grundlage einer Einwilligung erfolgen. Allerdings sind bei der Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit

---

69 Artikel-29-Datenschutzgruppe, WP 193, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, S. 13.

70 Artikel-29-Datenschutzgruppe, WP 259, Guidelines on Consent under Regulation 2016/679, S. 8. Der Europäische Datenschutzausschuss hat den auf die DS-GVO bezogenen Working Papers der Artikel-29-Datenschutzgruppe in seiner ersten Sitzung zugestimmt.

der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann danach insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Weder das eine noch das andere ist hier jedoch der Fall.

Eine wirksame Einwilligung in die Verarbeitung daktyloskopischer und damit biometrischer Daten scheidet jedenfalls dann aus, wenn nicht alternativ die Verwendung anderer Mittel der Zugangskontrolle, wie Chipkarte, PIN-Code oder Passwort, angeboten wird.

6.4.3
Fall 3: Biometrischer Lichtbildabgleich durch Skiliftbetreiber

Die Kunden einer Skiliftanlage werden beim Betreten der Anlage fotografiert. Die so erhobenen Gesichtsbilder werden mit Referenzfotos, welche beim Kauf des Skipasses erstellt wurden, automatisiert abgeglichen. Zweck der Verarbeitung ist die Verhinderung von Leistungserschleichungen in Gestalt einer missbräuchlichen Verwendung des Skipasses durch unberechtigte Dritte, die den Skipass entweder nur ausgeliehen oder durch privaten, günstigeren Weiterverkauf erworben haben.

Bei den jeweils angefertigten Fotografien handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO sowie aufgrund der abgebildeten Gesichter um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO. Die Aufnahmen werden biometrisch abgeglichen, um die betroffene Person eindeutig zu identifizieren. Als mögliche Rechtsgrundlage kommt Art. 9 Abs. 2 lit. f DS-GVO in Betracht. Danach ist eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist, sei es in einem gerichtlichen oder einem außergerichtlichen Verfahren.

Es stellt sich die Frage, ob ein automatisierter Abgleich hier wirklich erforderlich ist. Dabei ist zu berücksichtigen, dass ein solcher Abgleich die Grundrechte und Grundfreiheiten der betroffenen Personen erheblich beeinträchtigt. Wenn auch vereinzelt Leistungserschleichungen in Gestalt einer missbräuchlichen Verwendung des Skipasses durch unberechtigte Dritte auftreten, so ist dennoch in der Regel davon auszugehen, dass sich die überwiegende Mehrheit der Kunden rechtstreu verhält, also für eine solche Art von Kontrollen keinerlei Anlass bietet, es sei denn, dass konkrete Umstände im Einzelfall (z. B.

Nachweise über Missbräuche in nicht unerheblicher Zahl) die Erforderlichkeit einer solchen Maßnahme begründen können.

Vor diesem Hintergrund sollte dem Skiliftbetreiber die Durchführung etwa von Stichproben anhand der ausgegebenen Skipässe als milderes Mittel zuzumuten sein. Zu diesem Zweck kann der Skiliftbetreiber Skipässe verwenden, auf denen ab einer bestimmten Geltungsdauer ein Foto des Inhabers abgedruckt wird.

6.4.4
Fall 4: Zutrittskontrolle mit Handvenenscan für Flughafenmitarbeiter

Die F-GmbH betreibt zwei Flughäfen. Zur Sicherung des Flughafengeländes ist der Zugang zu den Sicherheitsbereichen nur berechtigten Personen gestattet. Die Zutrittsberechtigung wird durch die Vorlage des Flughafenausweises nachgewiesen. Darüber hinaus erfolgt eine zusätzliche biometrische Identitätsprüfung der Personen, die Zutritt zu den Sicherheitsbereichen des Flughafens haben, und zwar über das Verfahren der Handvenenbiometrie. Beim Einlesen der biometrischen Daten wird ein entsprechendes Handvenenmuster erstellt, welches auf dem Chip des Flughafenausweises in codierter Form hinterlegt wird. An den Kontrollstellen wird eine neue Handvenenaufnahme erstellt und mit der auf dem Chip des Ausweises gespeicherten Aufnahme verglichen. Der Handvenenscan bringe das derzeit höchste erreichbare Sicherheitsniveau bei der eindeutigen Identifizierung einer Person und sei auch als wirksame Abschreckung gegen jedweden Manipulationsversuch zu sehen, heißt es aus Flughafenkreisen.

Bei den Aufnahmen der Handvenenmuster handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO. Da diese für eine automatisierte biometrische Erkennung eingesetzt werden können, handelt es sich auch um biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO.

Die Verarbeitung der Aufnahmen der Handvenenmuster erfolgt im Sinne des Art. 9 Abs. 1 DS-GVO zur eindeutigen Identifizierung einer natürlichen Person. Die Identität des Ausweisinhabers soll zusätzlich durch den Vergleich der Handvenenaufnahmen überprüft werden.

Als Rechtsgrundlage für dieses Verfahren könnte Art. 9 Abs. 2 lit. g DS-GVO herangezogen werden. Danach ist eine Verarbeitung biometrischer Daten dann nicht untersagt, wenn sie aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist. An der Sicherheit des Flugverkehrs besteht ein erhebliches öffentliches Interesse.

Allerdings ist Art. 9 Abs. 2 lit. g DS-GVO kein eigenständiger Erlaubnistatbestand. Hinzutreten muss eine Rechtsgrundlage des Unionsrechts oder des Rechts eines Mitgliedstaats. In Betracht kommt hier § 8 Abs. 1 Nr. 4 Luftsicherheitsgesetz. Danach ist der Betreiber eines Flugplatzes zum Schutz des Flughafenbetriebs vor Angriffen auf die Sicherheit des Luftverkehrs verpflichtet, die Bereiche der Luftseite gegen unberechtigten Zugang zu sichern und, soweit es sich um Sicherheitsbereiche oder sensible Teile der Sicherheitsbereiche handelt, den Zugang nur hierzu besonders berechtigten Personen zu gestatten. Dem soll hier der Einsatz der Handvenenscanner dienen.

Die Verarbeitung muss allerdings zur Wahrung der Sicherheit des Flugverkehrs erforderlich sein. Zwar haben zwei Informatiker im Dezember 2018 gezeigt, wie sich Handvenenscangeräte überlisten lassen. Ein Einsatz dieser Technik unter organisatorisch abgesicherten Bedingungen und, wie hier, mit einer Zwei-Faktor-Authentisierung, wird vorliegend dennoch als zulässig erachtet, zumal gleich wirksame, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidende Mittel wohl nicht zur Verfügung stehen.

6.4.5
Fall 5: Zielgerichtete Außenwerbung durch biometrische Gesichtsanalyse

Ein Unternehmen betreibt ein System zur Außenwerbung. Dieses ermöglicht mithilfe von Sensoren an Informationsbildschirmen, biometrische Merkmale von Umstehenden zu erfassen und Alter und Geschlecht dieser Personen zu analysieren. Das Produkt dient dazu, die auf dem Bildschirm ausgegebenen Werbebotschaften an Alter und Geschlecht der umstehenden Personen anzupassen. Die an einem Bildschirm angebrachten Kamerasensoren erkennen und erfassen zunächst das Gesicht der Betrachtenden. Diese Bilder werden als Videostream temporär in einem Zwischenspeicher der Kamera abgelegt, bevor die darin verbaute Software sie in Histogramme umwandelt. Die Kamera verfügt zudem über einen Kalibriermodus, der eine Visualisierung der aufgezeichneten Bilder ermöglicht. Sonstige Übertragungen der Bilddaten finden nicht statt, es besteht auch keine Zugriffsmöglichkeit auf Bilddaten für das Unternehmen, Werbevertragspartner oder Dritte.

***Abwandlung:** Ein Unternehmen vertreibt eine Software zur Außenwerbung. Der Lizenznehmer installiert die Software auf seiner Hardware und bringt über dem Werbebildschirm eine von ihm selbst anzuschaffende, handelsübliche Videokamera an. Diese sendet einen Videostream an den Computer, wo die Software die erfassten Gesichter (Blick Richtung Kamera) sowie deren*

Bewegungsrichtung auswertet. Sodann werden die erfassten Gesichter mit Hilfe eines Algorithmus anhand biometrischer Merkmale (z. B. Behaarung, stark ausgeprägter Adamsapfel, Falten) ausgewertet. Nachdem die aufgenommene Person das Kamerafeld verlassen hat, wird das Ergebnis dieser Auswertung in einem Log File festgehalten. Die sich im RAM befindlichen Bild-Informationen werden mit dessen Erstellung automatisch gelöscht.

Bei den Videoaufnahmen handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO, auch wenn diese nur für einen sehr kurzen Zeitraum gespeichert werden.

Die Videoaufnahmen werden anhand biometrischer Merkmale ausgewertet. Allerdings erfolgt dies nicht zur eindeutigen Identifizierung der betroffenen Person, sondern vielmehr, um diese automatisch einer bestimmten Kategorie (u. a. Alter, Geschlecht) zuzuweisen. Die Rechtsgrundlage für diese Verarbeitung ist daher nicht in Art. 9 Abs. 2, sondern in Art. 6 Abs. 1 DS-GVO zu suchen.

Nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der hier verfolgte Zweck der Direktwerbung kann als eine einem berechtigten Interesse im Sinne von Art. 6 Abs. 1 lit. f DS-GVO dienende Verarbeitung betrachtet werden. In gleicher Weise geeignete Mittel zur Erfassung der Zielgruppengerechtigkeit der ausgespielten Werbespots dürften in der hier gelieferten Genauigkeit nicht zur Verfügung stehen.

Bei der nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO erforderlichen Abwägung ist entscheidend, ob die von der jeweils spezifischen Verarbeitungssituation ausgehenden Gefahren so groß und die bei ihrer Verwirklichung eintretenden Nachteile so erheblich sind, dass die Interessen der betroffenen Personen gegenüber denen des Verantwortlichen Vorrang beanspruchen können.[71] Je stärker das Maß der Beeinträchtigung durch die jeweilige Datenverarbeitung ist, desto „schutzwürdiger“ sind die Interessen der betroffenen Personen.[72]

Einerseits spricht insbesondere dafür, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen, dass hier durch die kurzzeitige Aufnahme von Gesichtsbildern und die Erfassung einzelner biometrischer Charakteristika grundsätzlich biometrische Daten verarbeitet werden. Die Verarbeitung biometrischer Charakteristika der Gesichter von Personen birgt erhebliche

71 Scholz, in Simitis, BDSG, § 6b Rn. 93.

72 Scholz, a. a. O., Rn. 94.

Sicherheitsrisiken und gegebenenfalls sind von einer Kompromittierung dieser Daten betroffene Personen lebenslangen Folgen eines Identitätsdiebstahls ausgesetzt, weil diese Daten nicht veränderbar sind.

Andererseits erhebt die eingesetzte Software nicht im ausreichenden Umfang Daten, um dauerhaft eine eindeutige Identifizierung der betroffenen Personen zu ermöglichen. Außerdem ist das für die betroffenen Personen bestehende Risiko aufgrund der relativ geringen Speicherdauer eher gering. Das gilt allerdings nur dann, wenn der Speicherzeitraum nicht verlängert werden kann, eine Identifizierung (d. h. eine Wiedererkennbarkeit) und Profilbildung der betroffenen Personen ausgeschlossen ist, die eingesetzte Software nicht dahingehend manipuliert werden kann, dass Daten erhoben werden können, die eine eindeutige Identifizierung ermöglichen, und die tatsächlich stattfindende Datenverarbeitung und ihr Zweck hinreichend transparent gemacht werden (Art. 13 Abs. 1 DS-GVO).

***Zur Abwandlung*:** Anders als im Ursprungsfall handelt es sich bei der Abwandlung nicht um ein geschlossenes System. Die in Gestalt der Videoaufnahmen erhobenen personenbezogenen Daten können länger gespeichert und zu anderen Zwecken, etwa zur eindeutigen Identifizierung der betroffenen Personen, weiterverwendet werden. Damit bewegen sich die in diesem Fall ergriffenen technischen und organisatorischen Maßnahmen auf einem deutlich niedrigeren Niveau, so dass im Ergebnis die Interessen der betroffenen Personen hier überwiegen. Die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO sind daher nicht erfüllt.

6.4.6
Fall 6: Zugangskontrolle auf Kreuzfahrtschiff

Auf einem Kreuzfahrtschiff wird beim Einchecken ein Foto angefertigt und gespeichert. Bei jedem Verlassen und Betreten des Schiffes wird die Chipkarte ausgelesen und der Fahrgast anhand des im System gespeicherten Fotos kontrolliert.

Wenn auf einem digitalen Bild gut erkennbar das Gesicht einer Person abgebildet ist, handelt es sich dabei um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO und zugleich um ein biometrisches Datum im Sinne des Art. 4 Nr. 14 DS-GVO, da es für eine automatisierte biometrische Erkennung eingesetzt werden kann.

Eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO liegt hier jedoch nicht vor. Die Bilder werden nicht zum Zweck der automatisierten biometrischen

Erkennung verarbeitet, sondern sollen bei einem manuellen Bildabgleich zum Einsatz kommen.

Als Rechtsgrundlage für die Verarbeitung kommt somit Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Der Reeder hat ein berechtigtes Interesse daran, dass nur Fahrgäste das Kreuzfahrtschiff betreten. Die Kontrolle beim Verlassen des Schiffes verschafft der Besatzung einen Überblick darüber, wer sich auf Landgang befindet. Beides entspricht auch dem Interesse der Fahrgäste, so dass die Verarbeitung als zulässig angesehen werden kann.

6.4.7
Fall 7: Videokamera in Juweliergeschäft

Der Inhaber eines Juweliergeschäfts installiert eine Videokamera und speichert die Aufnahmen für 48 Stunden. Er besitzt keine Software zur Gesichtserkennung, beabsichtigt aber im Falle einer Straftat die Weitergabe von Videoaufnahmen an die Polizei zum Zwecke der Identifikation von potenziellen Straftätern durch manuellen Bildvergleich und gegebenenfalls durch biometrische Verfahren.

Bei den Videoaufnahmen handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO. Videoaufnahmen insbesondere von Gesichtern können je nach Funktionalität der technischen Anlage grundsätzlich für eine Auswertung (z. B. Identifikation) anhand biometrischer Merkmale geeignet sein. Sie enthalten dann alle Informationen, die für eine solche Auswertung relevant sind.

Solche Videoaufnahmen sind daher als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen. Untersagt ist nach Art. 9 Abs. 1 DS-GVO lediglich eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person, also zum Zweck der automatisierten biometrischen Erkennung.

Eine solche Verarbeitung findet hier jedoch nicht statt, da der Juwelier nicht über ein biometrisches Identifikationssystem verfügt. Darunter versteht man ein System zum Zwecke der biometrischen Erkennung von Individuen anhand ihres Verhaltens oder ihrer biologischen Charakteristika.[73]

Auch ist zu bedenken, dass es nicht Sache des Juweliers ist, potenzielle Straftäter zu identifizieren. Dies ist die Aufgabe von Polizei und Staatsan-

73 ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV) as defined in SC37 Working Group 1 for the International Standard ISO/IEC 2382-37

waltschaft. Ihnen übergibt der Juwelier im Falle einer Straftat die Aufnahmen zur näheren Auswertung.

Als Rechtsgrundlage in Betracht kommt hier daher Art. 6 Abs. 1 S. 1 lit. f DS-GVO. Es kann dahingestellt bleiben, ob bei der Videoüberwachung durch Privatpersonen § 4 BDSG oder Art. 6 Abs. 1 S. 1 lit. f DS-GVO zur Anwendung kommt, da beide Vorschriften in vielen Fällen zu gleichen Ergebnissen führen. Nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die verfolgten Zwecke der Verhinderung von Straftaten einerseits sowie der Überführung von Straftätern andererseits können als berechtigte Interessen im Sinne des Art. 6 Abs. 1 S. 1 lit. f DS-GVO angesehen werden. Gleich wirksame, aber mit Blick auf die informationelle Selbstbestimmung der betroffenen Personen weniger einschneidende Mittel stehen wohl nicht zur Verfügung.

Bei der nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO erforderlichen Abwägung ist entscheidend, ob die von der jeweils spezifischen Verarbeitungssituation ausgehenden Gefahren so groß und die bei ihrer Verwirklichung eintretenden Nachteile so erheblich sind, dass die Interessen der betroffenen Personen gegenüber denen des Verantwortlichen Vorrang beanspruchen können.[74] Je stärker das Maß der Beeinträchtigung durch die jeweilige Datenverarbeitung ist, desto „schutzwürdiger" sind die Interessen der betroffenen Personen.[75]

Dafür, dass die schutzwürdigen Interessen der betroffenen Personen überwiegen, spricht die hier erfolgende Aufnahme und Speicherung von Gesichtsbildern sowie deren grundsätzliche Eignung zur eindeutigen Identifizierung natürlicher Personen. Die sich daraus ergebenden Risiken für die Rechte und Freiheiten der betroffenen Personen muss der Verantwortliche durch technische und organisatorische Maßnahmen minimieren. Zu Gunsten des Verantwortlichen kann die Abwägung jedoch nur dann ausgehen, wenn er sicherstellt, dass eine Speicherdauer von 48 bis maximal 72 Stunden nicht überschritten wird, dass auf seiner Hardware keine Gesichtserkennungssoftware installiert und genutzt wird und dass die stattfindende Datenverarbeitung sowie deren Zwecke den betroffenen Personen hinreichend transparent gemacht werden (Art. 13 Abs. 1 DS-GVO).

74 Scholz, a. a. O., Rn. 93.

75 Scholz, a. a. O., Rn. 94.

6.4.8
Fall 8: VIP-Gast-Erkennung in Hotels

Ein Hotel benutzt eine Videoüberwachungsanlage mit Gesichtserkennungssystem, das den Hotelmanager auf angekommene VIP-Gäste aufmerksam macht. Aufnahmen dieser VIP-Gäste wurden zuvor mit deren Einverständnis in eine Datenbank aufgenommen. Allerdings werden auch von allen anderen Gästen Videoaufnahmen gemacht, Templates erstellt und mit dem Inhalt der Datenbank verglichen.

Wenn auf einem digitalen Bild klar sichtbar das Gesicht einer Person abgebildet ist, handelt es sich dabei um ein personenbezogenes Datum im Sinne des Art. 4 Nr. 1 DS-GVO. Die hier mit Hilfe der Videoüberwachungsanlage verarbeiteten Gesichtsbilder sind zudem als biometrische Daten im Sinne des Art. 4 Nr. 14 DS-GVO einzustufen, da sie für eine automatisierte biometrische Erkennung eingesetzt werden können.

Die Verarbeitung der Videoaufnahmen erfolgt auch zum Zwecke der eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO. Der Hotelmanager möchte auf angekommene VIP-Gäste aufmerksam gemacht werden, diese namentlich ansprechen können und von nicht als VIPs eingestuften Gästen unterscheiden.

Die Verarbeitung betrifft alle Personen, die den Eingangsbereich des Hotels betreten, also als VIPs registrierte und nicht registrierte Gäste. Zweck der Verarbeitung ist eine biometrische Erkennung. Von allen Gästen werden digitale Gesichtsbilder erstellt. Aus den Gesichtsbildern werden biometrische Merkmale extrahiert und mit den in der hoteleigenen Datenbank vorhandenen Daten verglichen. Darauf, ob sich als Ergebnis dieses Vergleichs ein Trefferfall ergibt oder nicht, kommt es für den Zweck der Verarbeitung nicht an. Theoretisch kann jede Person, die den Eingangsbereich des Hotels betritt, ein VIP-Gast sein. Die Einbeziehung der Daten auch von Personen, deren Vergleich letztlich zu Nichttreffern führt, ist notwendiger und gewollter Teil des Verfahrens und gibt diesem erst seinen Sinn.

Für die Verarbeitung der Gesichtsbilder der bereits als VIPs registrierten Gäste kann gemäß Art. 9 Abs. 2 lit. a DS-GVO deren ausdrückliche Einwilligung herangezogen werden. Für die Verarbeitung der Gesichtsbilder der anderen Gäste ist eine Rechtsgrundlage nicht ersichtlich. In seiner derzeitigen Gestalt lässt sich das Verfahren somit nicht in Einklang mit der DS-GVO bringen.

7.
Auswahl von Maßnahmen und Schlussfolgerungen für die Verfahrensgestaltung

7.1
Modell und Grundannahmen

7.1.1
Methodik

Da die Verarbeitung personenbezogener Daten immer ein Risiko für die Rechte und Freiheiten betroffener Personen darstellt, sind die Verantwortlichen dazu verpflichtet, die Grundsätze aus Art. 5 DS-GVO einzuhalten. Die getroffenen Maßnahmen sind nach Art. 5 Abs. 2 DS-GVO zu dokumentieren. Die Nicht-Einhaltung der in Art. 5 verankerten Grundsätze kann gemäß Art. 83 Abs. 5 lit. a DS-GVO mit einem Bußgeld geahndet werden.

Um diese Grundsätze einhalten zu können, müssen gemäß Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Verantwortliche und Auftragsverarbeiter haben die jeweiligen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen auszuwählen. Biometrische Daten erfordern in aller Regel eine besondere Aufmerksamkeit, da eine Einzelperson unwiderruflich mit ihnen verbunden ist und anhand dieser Daten aufgrund ihrer individuellen verhaltensbezogenen oder physiologischen Merkmale zweifelsfrei identifiziert werden kann.

Das von den unabhängigen Datenschutzbehörden des Bundes und der Länder entwickelte Standard-Datenschutzmodell (SDM) bietet geeignete Hilfestellungen, um die rechtlichen Anforderungen der DS-GVO in konkrete technische und organisatorische Maßnahmen zu überführen, auch wenn die Arbeit an einzelnen Teilen derzeit noch nicht abgeschlossen ist. Das SDM strukturiert die rechtlichen Anforderungen in Form der folgenden Gewährleistungsziele: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit. Diese Anforderungen zielen auf Eigenschaften einer rechtskonformen Verarbeitung, die durch technische und organisatorische Maßnahmen „gewährleistet“ werden müssen. Die Gewährleistung besteht im Ausschluss von Abweichungen von einer rechtskonformen Verarbeitung. Durch diese Gewährleistungsziele werden die rechtlichen Anforderungen der DS-GVO in die von der Verordnung geforderten technischen und organisatorischen Maßnahmen überführt. Das SDM enthält eine Auflistung generischer technischer und organisatorischer

Maßnahmen. Mit Hilfe dieses generischen Katalogs kann bei jeder einzelnen Verarbeitung sowohl durch den Verantwortlichen selbst als auch durch die Aufsichtsbehörde geprüft werden, ob die vor Ort vorhandenen Maßnahmen das rechtlich geforderte Soll von Maßnahmen erfüllen.[76]

Wegen der Vielfalt der betrachteten Systeme ist eine vollständige und detaillierte Darstellung der Risiken und angemessenen zu ergreifenden technischen und organisatorischen Maßnahmen im Rahmen des vorliegenden Papiers nicht möglich. Um die Grundsätze der Datenverarbeitung gemäß Art. 5 DS-GVO einhalten zu können, müssen Verantwortliche ihre Systeme individuell untersuchen.

7.1.2
Systemaufbau

In einem ersten Schritt ist zunächst das zur Anwendung kommende System zu analysieren. Die Untersuchung eines Systems erfordert zunächst die Bestimmung der Systemgrenzen und der grundlegenden Struktur des Systems. Systeme zur Verarbeitung biometrischer Daten, wie sie im vorliegenden Papier vorgestellt werden, bestehen typischer Weise aus den folgenden Komponenten:

– biometrische Erfassungsgeräte
– Verarbeitungslogik (führt insbesondere die biometrische Merkmalsextraktion und die biometrische Erkennung durch)
– Aktor(en) (an die Verarbeitungslogik angeschlossene Ausgabegeräte)
– Referenzdatenbank, Enrolmentdatenbank
– weitere Eingabeschnittstellen
– weitere Ausgabeschnittstellen
– Wartungsschnittstellen
– Verbindungen zwischen den Komponenten

Sodann sind die an der Verarbeitung beteiligten Akteure zu identifizieren. Akteure, die einen Einfluss auf die Verarbeitung der Daten im System haben oder haben können, sind in der Regel:

– Systembetreiber
– Betroffene
– Wartungsunternehmen

76 Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S. 5.

– Hersteller
– ggf. Stellen, die dem System Daten zur Verfügung stellen oder Daten aus ihm erhalten

Daneben müssen auch solche Akteure betrachtet werden, die ein Interesse an einer nicht bestimmungsgemäßen Verarbeitung von Daten in oder aus dem System haben könnten. Dies ist erforderlich, um prüfen zu können, ob die Sicherheitsmaßnahmen, die der Verantwortliche ergriffen hat, die Betroffenen auch hinreichend stark gegen Missbrauch schützen. Hierbei werden sowohl persönliche als auch wirtschaftliche oder politische Motive zu berücksichtigen sein. Abbildung 2 – Überblick über typische Komponenten biometrischer Systeme zeigt die Akteure und Komponenten biometrischer Systeme und ihre Verbindungen.

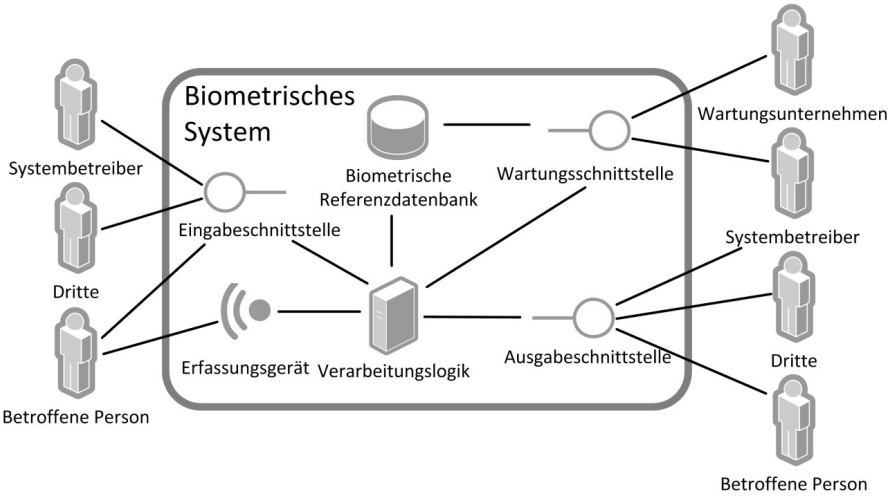

Abbildung 2 – Überblick über typische Komponenten biometrischer Systeme

Nicht in allen Systemen findet sich jede der genannten Komponenten. So entfällt die Referenzdatenbank bei der Reichweitenmessung und in Authentifizierungsverfahren kann die Referenzdatenbank auf einen Datensatz beschränkt sein, wenn beispielsweise die Identität einer Person ausschließlich anhand der in einem Ausweisdokument gespeicherten Daten überprüft wird. Die Wartungsschnittstelle wird hingegen in der Regel zu berücksichtigen sein: Eingebettete Systeme enthalten eine solche Schnittstelle zu Zwecken der Programmierung und der Diagnose; auf offenen Systemen wie PC-Technik

basierte Lösungen gestatten problemlos den Einsatz von Fernwartungstechnik oder haben entsprechende Komponenten bereits vorinstalliert.

7.1.3
Überblick über die für biometrische Systeme typischen Verarbeitungen

Gemäß der zuvor betrachteten biometrischen Systeme und Fallbeispiele können im Wesentlichen drei Arten von biometrischen Systemen unterschieden werden, die jeweils unterschiedliche Risiken für die Rechte und Freiheiten Betroffener mit sich bringen:

– Systeme zur biometrischen Suche,
– Systeme zum biometrischen Vergleich oder
– Systeme zur biometrischen Eigenschaftsableitung.

Derzeit haben praktisch relevante biometrischen Systeme gemein, dass eine Erfassung biometrischer Charakteristika betroffener Personen in der Form biometrischer Samples erfolgt und aus diesen biometrische Merkmale extrahiert werden. Verfahren zur biometrischen Suche bedürfen darüber hinaus, dass biometrische Daten in einer Datenbank (in der Regel zusammen mit zusätzlichen Daten) erfasst werden, das sogenannte Enrolment. Somit können im Wesentlichen sechs verschiedene Arten von Verarbeitungen differenziert werden (Erfassung, Merkmalsextraktion, Enrolment, Suche, Vergleich und Eigenschaftsableitung).

Bei der biometrischen Erfassung nimmt ein biometrisches Erfassungsgerät ein biometrisches Charakteristikum einer betroffenen Person in Form eines biometrischen Samples auf.

Zur weiteren Verarbeitung der aufgenommenen biometrischen Samples müssen aus diesen biometrische Merkmale extrahiert werden. Abhängig davon, ob das biometrische System biometrische Merkmale oder biometrische Samples verwendet, erfolgt dieser Verarbeitungsschritt direkt nach der biometrischen Erfassung oder die Merkmalsextraktion ist Teil der Verarbeitungslogik (Enrolment, Suche, Vergleich oder Eigenschaftsableitung).

Beim Enrolment wird eine biometrische Probe (Sample oder Merkmal) als biometrische Referenz zusammen mit weiteren Daten der betroffenen Person, die über eine entsprechende Eingabeschnittstelle erhoben werden, in einer biometrischen Referenzdatenbank gespeichert.

Bei der biometrischen Suche wird geprüft, ob eine gegebene biometrische Probe mit biometrischen Referenzen in der biometrischen Referenzdatenbank übereinstimmt und es wird eine Liste möglicher Kandidaten an eine Ausgabeschnittstelle gegeben.

Im Vergleich zur biometrischen Suche wird beim biometrischen Vergleich lediglich geprüft, zu welchem Grad eine gegebene biometrische Probe mit einer biometrischen Referenz übereinstimmt und der entsprechende Vergleichswert wird an eine Ausgabeschnittstelle weitergeleitet.

Bei der biometrischen Eigenschaftsableitung werden aus einem biometrischen Sample biometrische Eigenschaften berechnet und an eine Ausgabeschnittstelle weitergegeben. Die biometrischen Samples können dabei von einem biometrischen Erfassungsgerät, über eine Eingabeschnittstelle oder aus einer biometrischen Referenzdatenbank stammen.

Sollten zukünftige Verfahren, die, beispielsweise unterstützt durch Künstliche Intelligenz, auf eine andere Art eine biometrische Erkennung durchführen, müssten die dabei durchgeführten Verarbeitungsschritte nach den Vorgaben dieses Papiers gesondert betrachtet werden.

7.2
Risiken

Um ein angemessenes Schutzniveau gewährleisten zu können, muss der Verantwortliche die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen identifizieren.

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Aus den Erwägungsgründen 75 und 94 Satz 2 DS-GVO kann folgende Definition hergeleitet werden: Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich einer ungerechtfertigten Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.[77]

Die DS-GVO gibt dem Verantwortlichen im Erwägungsgrund 76 zwei Stufen zur Bestimmung des Risikos einer personenbezogenen Verarbeitungstätigkeit vor, nämlich „Risiken“ und „hohe Risiken“. Zur Feststellung der Risikostufe sind die Art, der Umfang, die Umstände und die Zwecke der Verarbeitungstätigkeit sowie die spezifischen Eintrittswahrscheinlichkeiten und Schwere der Risiken bei der jeweiligen Verarbeitungstätigkeit zu berücksichtigen.

Speziell bei der Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person müssen die spezifischen Risiken betrachtet

77 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 1.

werden, die sich allein aus diesem Umstand ergeben.[78] Zur Identifikation von Datenschutzrisiken bietet es sich an, von folgenden Fragen auszugehen:

– Welche Schäden können für die natürlichen Personen auf der Grundlage der zu verarbeitenden Daten entstehen?
– Wodurch, d. h. durch welche Ereignisse kann es zu einem Schaden kommen?
– Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?[79]

In den hier betrachteten Verfahren werden überwiegend biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person im Sinne des Art. 9 Abs. 1 DS-GVO verarbeitet. Ungeachtet der Eintrittswahrscheinlichkeit eines möglichen Schadens kann zumindest regelmäßig von einer besonderen Schwere des Schadens ausgegangen werden. Dies ergibt sich bereits aus dem Umstand, dass es sich teilweise um die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO handelt, bei denen die DS-GVO einen gesteigerten Schutzbedarf vorsieht. Der Schaden dürfte außerdem nicht oder kaum reversibel sein, da die Identität einer natürlichen Person, wie eingangs bereits erwähnt, unwiderruflich und untrennbar mit ihren biometrischen Daten verbunden ist. Die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung natürlicher Personen ist daher ein wichtiges Indiz für ein „hohes Risiko“ im Sinne des Erwägungsgrundes 76.[80] Das Kurzpapier Nr. 18 der DSK zum Thema „Risiko für die Rechte und Freiheiten natürlicher Personen“ bietet für die Abschätzung des Risikos eine Matrix an, die Verantwortliche zur Feststellung des Risikos bei der von ihnen beabsichtigten Verarbeitungstätigkeit heranziehen können. Sollten Verantwortliche zu dem Ergebnis kommen, dass die von ihnen beabsichtigte Verarbeitungstätigkeit voraussichtlich ein „hohes Risiko“ für die Rechte und Freiheiten natürlicher Personen darstellt, ist die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO notwendig.

78 Europäischer Datenschutzausschuss: Working Paper 193 „Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien“, S. 5.

79 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 2.

80 Siehe auch: Europäischer Datenschutzausschuss: Working Paper 248 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA)“

7.3
Maßnahmen

Folgt man der Systematik des Standard-Datenschutzmodells, müssen die eingangs erwähnten Gewährleistungsziele (Sicherung der Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit) auch bei der Verarbeitung biometrischer Daten bzw. bei der Nutzung biometrischer Verfahren erreicht werden. Dabei sind die spezifischen Risiken, die mit dem Einsatz biometrischer Verfahren und der Verarbeitung biometrischer Daten verbunden sind, zu berücksichtigen. Jedes der Gewährleistungsziele kann durch bestimmte technische und organisatorische Maßnahmen erreicht werden, die im Standard-Datenschutzmodell zumindest in generischer Form beschrieben sind.[81] Neben den im SDM verschriftlichten generischen Maßnahmen zur Umsetzung der Gewährleistungsziele ist eine weitere Komponente zu beachten, sofern für eine beabsichtigte Verarbeitungstätigkeit ein „hohes Risiko" für die Rechte und Freiheiten der betroffenen Personen festgestellt wurde. Ein „hohes Risiko" entspricht einem „hohen Schutzbedarf" und führt zu Maßnahmen mit entsprechend höheren Anforderungen an deren Wirksamkeit oder erfordert sogar zusätzliche Maßnahmen.[82] Konkret bedeutet dies, dass jede der getroffenen Schutzmaßnahmen wiederum selbst anhand der Gewährleistungsziele beurteilt werden muss. Wenn z. B. das Gewährleistungsziel „Vertraulichkeit" in einem biometrischen System erreicht werden soll, indem ein Rechte- und Rollenkonzept nach dem Erforderlichkeitsprinzip festgelegt wird, so muss dieses Rechte- und Rollenkonzept selbst verfügbar, integer, vertraulich, nichtverkettbar, transparent und intervenierbar sein. Oder, um noch ein weiteres Beispiel zu nennen: Bei hohem Risiko reicht es nicht, Aktivitäten des Systems zu protokollieren; die Protokolldaten müssen ihrerseits verfügbar sein, die Revisionsfestigkeit kann z. B. durch die Verwendung von Signaturen gesichert werden, es gilt zu überlegen, ob Protokolldaten nur verschlüsselt gespeichert werden usw. Entscheidend ist zudem, dass bei hohen Risiken nach dem SDM ein Datenschutzmanagement-System zu betreiben ist, das dafür sorgt, dass festgestellte Schwächen und Mängel auch nachhaltig behoben werden können.

---

81 Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S.22 ff.

82 Standard-Datenschutzmodell (SDM), Version 1.1, verabschiedet von der 95. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 26. April 2018, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf, S.32.

7.4
Restrisiko

Nach der Auswahl von technischen und organisatorischen Maßnahmen und deren Umsetzung muss das verbleibende Risiko für die betroffenen Personen beurteilt werden. Ergibt sich nach Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO ein hohes Restrisiko, muss die zuständige Aufsichtsbehörde konsultiert werden (Art. 36 DS-GVO).[83]

83 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, S. 6.

3.9 „Whitepaper“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder 07. November 2019

Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich

Messenger-Dienste haben parallel zur Verbreitung von Smartphones in den letzten Jahren zentrale Bedeutung für den Austausch von Nachrichten erlangt, andere Kommunikationsdienste wie E-Mail oder SMS vielfach ersetzt und zählen im privaten Alltag zu den beliebtesten Kommunikationsformen.

Gründe hierfür sind neben der jederzeitigen Nutzbarkeit über Smartphone und der leichten Bedienbarkeit der Funktionsumfang, der es erlaubt, neben Textnachrichten auch Bilder, Videos oder Sprachnachrichten auszutauschen, Sprach- und Videoanrufe durchzuführen und wahlweise mit einzelnen Teilnehmern oder in der Gruppe zu kommunizieren. Hinzu kommt, dass es sich vielfach um unentgeltlich nutzbare Angebote handelt.

Aufgrund der im privaten Bereich weitverbreiteten und etablierten Nutzung wird auf diese Messenger-Dienste zunehmend auch im Gesundheitsbereich zurückgegriffen, häufig verbunden mit der Nutzung eines privaten Endgeräts.[84,85,86]

Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutz-Vorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen. Insbesondere der verbreitet genutzte Dienst WhatsApp führt bei einer geschäftlichen Nutzung zu einer Reihe von Problemen[87], die einen Einsatz im Krankenhaus weitgehend ausschließen. Ähnliches gilt für andere im privaten Bereich häufig genutzte Dienste.

Mit Blick auf die Sensibilität der im Gesundheitsbereich betroffenen Daten und den besonderen Schutz, den diese nach Art. 9 Datenschutz-Grundverordnung (DS-GVO) genießen, sind daher bei der Auswahl geeigneter Messenger-Dienste für die Übermittlung von Patientendaten im Krankenhausbereich vom Verantwortlichen die nachfolgenden Datenschutzanforderungen zu berücksichtigen. Die daraus ableitbaren Vorgaben dienen gleichzeitig als

84 https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/902262/klinik-jeder-dritte-arztverschickt-patientendaten-via-apps.html

85 https://www.kardiologie.org/kardiologie/whatsapp-und-co--wissen-aerzte--was-sie-tun-/15742284

86 https://deutsches-datenschutz-institut.de/wp-content/uploads/2018/05/FAZ_Messenger-2018.pdf

87 https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/

Orientierung für den Einsatz von Messenger-Diensten im niedergelassenen Bereich.

Ein Einsatz von Messenger-Diensten im Krankenhausbereich kann in unterschiedlichen Szenarien erfolgen (z. B. krankenhausinterne Nutzung, Konsil, Kommunikation mit Rettungsdiensten, Kommunikation mit Arztpraxen, Kommunikation mit anderen Leistungserbringern, Kommunikation mit Patienten). Je nach Szenario können sich dabei unterschiedliche Anforderungen ergeben.

Die nachfolgenden Anforderungen beziehen sich vorrangig auf die eigentliche Messenger-Applikation, die Kommunikation zwischen den Teilnehmern, die genutzte Plattform sowie die eingesetzten Endgeräte. Der eigentliche Betrieb von Messenger-Diensten im Krankenhaus findet nur insoweit Berücksichtigung, als es sich um allgemeine Anforderungen handelt. Nicht betrachtet werden in diesem Papier aufgrund der Heterogenität der Einsatzbedingungen funktionale Anforderungen des Krankenhausbetriebs einschließlich gebotener technischer und organisatorischer Vorkehrungen.

Erhebliche Risiken“, wie es die DS-GVO formuliert, sind bei der Verarbeitung von in Art. 9 DS-GVO genannten Datenkategorien wie Gesundheitsdaten oder genetische Daten immer anzunehmen. Dabei liegt der Schutzbedarf in den personenbezogenen Daten selbst. Wenn in diesem Papier die Verarbeitung in einem Krankenhaus angesprochen wird, dann deshalb, weil die datenschutzrechtlichen Anforderungen sich grundsätzlich an „den“ Verantwortlichen (i. S. v. Art. Ziff. 7 DS-GVO) richten und in Krankenhäusern i. d. R. immer auch eine umfangreiche Verarbeitung personenbezogener Daten erfolgt.

Soweit der nachfolgende Text Muss-Anforderungen formuliert, sind diese datenschutzrechtlich geboten und müssen deshalb zwingend umgesetzt werden. Soll-Anforderungen können dagegen verschiedene Ausprägungen haben: Sofern es zur Sicherstellung des Datenschutzes gleichwertige Handlungsalternativen gibt, reicht es aus, wenn eine davon realisiert wird. Dabei bleibt es dem Verantwortlichen im Rahmen der durch Art. 24 Abs. 1, Art. 32 Abs. 1 DS-GVO eröffneten Spielräume überlassen, welche der Möglichkeiten er tatsächlich auswählt. Darüber hinaus können Sollte-Anforderungen einen aus der Sicht des Datenschutzes zwar wünschenswerten, rechtlich aber nicht zwingend gebotenen Umstand beschreiben. Hier entscheidet der Verantwortliche selbst, ob er der Anforderung nachkommt.

I.
Messenger-Applikation

1. Die Applikation muss die Möglichkeit bieten, die Nutzerinnen und Nutzer entsprechend Art. 13 DS-GVO über die mit der Nutzung verbundene Datenverarbeitung zu unterrichten. Die Informationen müssen in einem klar erkennbaren Bereich (z. B. Hinweise zum Datenschutz, Datenschutzerklärung) für den jederzeitigen Zugriff hinterlegt sein.
2. Die Applikation muss über die Möglichkeit verfügen, die Nutzung bzw. den Zugriff auf die darüber gespeicherten Daten an eine eigene vorherige Authentifizierung (z. B.
3. PIN, Fingerabdruck etc.) zu knüpfen. Diese kann auf betriebssystemseitige Funktionen zurückgreifen, muss sich jedoch vom Schutz zur Entsperrung des Mobilgeräts (siehe III.1) unterscheiden.
4. Die Applikation muss über die Möglichkeit verfügen, Kontaktdaten von Kommunikationsteilnehmern in einem eigenen, vom allgemeinen Adressbuch des Smartphones getrennten Speicher abzulegen. Sie sollte in diesem Zusammenhang über eine Möglichkeit verfügen, Kontakte und zugehörige Informationen aus anderen Quellen importieren zu können. Sie muss weiterhin über die Möglichkeit verfügen, Nachrichten sowie Dateianhänge wie Bilder, Videos, Dokumente etc. ausschließlich in einem eigenen, von den allgemeinen Speicherbereichen des Smartphones getrennten Speicher in verschlüsselter Form abzulegen. Dabei kann auf betriebssystemseitig vorhandene kryptografische Funktionen zurückgegriffen werden. Die Applikation sollte über die Möglichkeit verfügen, Nachrichten und Dateianhänge aus anderen Quellen zu importieren.
5. Die Applikation sollte die Möglichkeit bieten, für die serverseitige Authentifizierung, Verschlüsselung oder digitale Signatur benötigte Daten (z. B. Zertifikate, Schlüssel) zu importieren. Eine Kommunikation über die Messenger-Applikation sollte nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.
6. Werden elektronische Signaturen oder andere elektronischer Zertifikate genutzt, muss ein Zertifikatsmanagement vorhanden sein. Dies beinhaltet die Sicherstellung, dass elektronische Schlüssel oder Zertifikate eindeutig einer juristischen oder natürlichen Person zugeordnet werden, aber auch die Überprüfung der Gültigkeit der elektronischen Schlüssel bzw. Zertifikate. Insbesondere müssen kompromittierte Schlüsseln bzw. Zertifikate unbrauchbar gemacht werden können. Dabei ist unerheblich, ob das Management der genutzten Public Key Infrastructure („PKI“)

vom Verantwortlichen selbst betrieben wird oder von einem Dritten zur Verfügung gestellt wird.

7. Die Applikation sollte über eine Schnittstelle verfügen, die es erlaubt, sie in IT-Strukturen und -Prozesse eines Krankenhauses einzubinden (z. B. Aufspielen von Sicherheitsprofilen oder Voreinstellungen, Synchronisation mit dem Krankenhausinformationssystem, Übernahmen behandlungsrelevanter Messenger-Nachrichten als Teil der Patientendokumentation).
8. Die Applikation muss über die Möglichkeit verfügen, die über sie verwalteten Daten gezielt oder allgemein zu löschen (Nachrichten, Dateien, Kontakte etc.). Sie sollte über die Möglichkeit verfügen, eine Frist festzulegen, nach der solche Daten automatisiert gelöscht werden.
9. Soweit im Rahmen der Nutzung der Applikation Dienste Dritter zur Fehleranalyse eingebunden werden (z. B. Crashlytics), muss dies offen erkennbar dargestellt und als optional gekennzeichnet werden; die für eine Übermittlung zur Fehlersuche vorgesehenen Datenkategorien müssen klar erkennbar sein. Eine entsprechende Datenübermittlung muss in der Voreinstellung deaktiviert sein. Es muss sichergestellt sein, dass Daten, die dem Arztgeheimnis unterliegen, oder Daten über das Nutzungsverhalten der Messenger-Anwender auf diese Weise nicht unbefugt offenbart werden.
10. Mit Blick auf die Verfügbarkeit der Daten nach Art. 32 Abs. 1 lit. b DS-GVO muss die Applikation über die Möglichkeit einer Sicherung der Kontaktdaten/Inhaltsdaten/Kommunikationsvorgänge verfügen. Soweit die Speicherung unter Einhaltung von Art. 28 DS-GVO durch einen Dienstleister übernommen wird, welcher nicht die Anforderungen des Art. 9 Abs. 3 DS-GVO erfüllt, muss die Möglichkeit bestehen, die Daten nach dem Stand der Technik vor ihrer Übergabe derart zu verschlüsseln, dass eine Entschlüsselung nur mit einem Schlüssel möglich ist, der nicht an den Dienstleister offenbart und separat gesichert wird. Dabei ist eine Sicherung zur Gewährleistung der Verfügbarkeit aus datenschutzrechtlichen Gründen von der Speicherung zu Dokumentationszwecken abzugrenzen. Die aus berufsrechtlicher Sicht einschlägige ärztliche Dokumentationspflicht (vgl. § 10 MBO-Ä, § 630f BGB) bleibt davon unberührt; sie darf bei einem Einsatz von Messengern nicht vernachlässigt werden. Eine Dokumentation, die (teilweise) im Messenger erfolgt und in der Patientendokumentation nicht nachvollziehbar ist, muss unterbleiben. Behandlungsrelevante Inhaltsdaten, die sich auf Patienten beziehen und auf dem Endgerät erzeugt werden (z. B. durch Kameraaufnahmen), müssen in der IT-Struktur des Krankenhauses gespeichert und über die Behandlungsdokumentation auffindbar sein können, soweit dies aus berufs- oder zivilrechtlicher Sicht geboten ist.

Hierzu bedarf es nicht notwendigerweise einer speziellen, an das KIS angepassten Funktion in der Messenger-Applikation, solange sich der Prozess anderweitig effizient abbilden lässt. Vorgaben des Berufs- und Zivilrechts bleiben unangetastet.

11. Soweit über die Applikation Bildaufnahmen verschickt werden (z. B. Patientenaufnahmen, Screenshots), bei denen darin enthaltene personenbezogene Daten für den verfolgten Zweck und die Identität aus ärztlicher Sicht nicht erforderlich sind, und die Patientenidentität vor dem Hintergrund einer sorgfältigen Behandlung ausnahmsweise verzichtbar ist, soll die Möglichkeit bestehen, Teile der Aufnahmen zu schwärzen oder anderweitig in der Darstellung auszunehmen (Datenminimierung, vgl. Art. 5 Abs. 1 lit. c, Art. 25 Abs. 1 DS-GVO).
12. Für die Messenger-Lösung ist durch das Krankenhaus und ggf. den beauftragten Auftragsverarbeiter ein geeigneter Nachweis darüber zu führen, dass die für die Erfüllung der Datenschutz-Grundsätze und die Gewährleistung der Sicherheit der Verarbeitung nach Art. 25 Abs. 1 bzw. 32 DS-GVO enthaltenen Funktionen effektiv implementiert wurden bzw. bei den jeweiligen Verarbeitungsvorgängen die Vorgaben der DS-GVO eingehalten werden (z. B. Zertifizierung nach Art. 42 DS-GVO (soweit verfügbar), Zertifizierung nach European Privacy Seal, BSI-Grundschutz-Zertifizierung). Seitens des Krankenhauses sollte die Messenger-Applikation zudem anhand des Prüfkatalogs zum technischen Datenschutz bei Apps[88] bewertet und das Ergebnis im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) dokumentiert werden.
13. Die Applikation muss hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen.
14. Die Applikation soll über (halb-)automatische Update-Verfahren verfügen.

II.
Kommunikation

1. Die Vertraulichkeit und Integrität der über den Messenger-Dienst geführten ärztlichen Kommunikation muss unter Berücksichtigung des Stands der Technik über eine Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationsteilnehmern gewährleistet werden (Art. 32 Abs. 1 lit. a DS-GVO).

88 https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

2. Soweit die Integrität der über den Messenger-Dienst kommunizierten Daten für nachfolgende Maßnahmen von Bedeutung ist, sollte die Möglichkeit bestehen, diese durch kryptografische Funktionen unter Berücksichtigung des Stands der Technik nachzuweisen (Art. 32 Abs. 1 Satz 1 DS-GVO). Weiterhin muss zur Gewährleistung der Integrität der Informationen, wenn diese für nachfolgende Maßnahmen von Bedeutung ist, dafür Sorge getragen werden, dass alle kommunizierten Daten beim Empfänger ankommen. Wird eine Mitteilung seitens eines Messengers auf mehrere Nachrichten verteilt (z. B. weil der Messenger pro Nachricht nur eine bestimmte Zeichenzahl oder Dateigröße zulässt), müssen Mechanismen integriert sein, die dem Empfänger mitteilen, ob die gesendete Mitteilung vollzählig angekommen ist oder ob einzelne Nachrichten fehlen. Dies kann z. B. durch die Ergänzung einer Prüfnummer „Nachricht x von y" geschehen, so dass der Empfänger sieht, ob alle Nachrichten bei ihm angekommen sind.
3. Verbindungsdaten zu der über den Messenger-Dienst geführten Kommunikation (z. B. Kommunikationsteilnehmer, Zeitpunkt, Geräte- und Standortdaten) dürfen nur solange und soweit gespeichert werden, wie es für die Übermittlung von Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist. Die Kommunikations- bzw. Metadaten dürfen ausschließlich für eigene Zwecke des Krankenhauses genutzt werden. Eine Nutzung für andere Zwecke durch den Hersteller der Lösung oder den Plattformbetreiber (z. B. Werbezwecke) ist unzulässig.
4. Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle (z. B. XMPP[89]) möglich sein, um eine Kommunikation mit anderen Messenger-Diensten zu ermöglichen.

III.
Sicherheit der Endgeräte

1. Die eingesetzten Endgeräte müssen über einen wirksamen Zugriffsschutz verfügen (z. B. PIN/Passphrase, biometrische Lösungen). Der interne Speicher der Geräte muss durch Verschlüsselung so geschützt werden, dass eine Entschlüsselung die Kenntnis der Anmeldedaten voraussetzt.
2. Es dürfen lediglich Geräte zum Einsatz kommen, deren Betriebssystemversion durch den Hersteller der Betriebssystemplattform (Google bzw. Apple) aktuell mit Sicherheitspatches versorgt werden und bei denen alle

89 Extensible Messaging and Presence Protocol (XMPP) der IETF, als Protokollstandard RFC 6120, 6121 und 6122 veröffentlicht: https://tools.ietf.org/html/rfc6122

derartigen Sicherheitspatches angewandt wurden. Dies setzt voraus, dass die Hersteller der Endgeräte eine ggf. erforderliche Anpassung auf den jeweiligen Gerätetyp unverzüglich vornehmen.

3. Die Endgeräte müssen einem Dienst für das Mobile Device Management (MDM) unterworfen werden, welches durch eine sichere Konfiguration der Geräte und Datenverbindungen das Risiko
   a. des Einschleusens von Schadcodes (u. a. über Schwachstellen der Browser, Dateibetrachter, Betriebssystemplattform und Schnittstellen des Geräts),
   b. des unbefugten Zugangs von Dritten auf das Gerät selbst und auf die verarbeiteten Daten

   minimiert, eine Verarbeitung unterbindet, wenn das Betriebssystem des Geräts nicht die unter 2 genannten Eigenschaften aufweist, die Anwendung von Sicherheitspatches und Aktualisierungen anstößt und die Installation von Apps überwacht. Der Dienst sollte ebenso eine Ortung und Sperrung oder Löschung der Geräte bei Verlust ermöglichen, wobei jedoch eine permanente Lokalisierung der Besitzer auszuschließen ist.

IV.
Plattform/Betrieb

1. Soweit es sich bei dem in Anspruch genommenen Messenger-Dienst um einen öffentlich zugänglichen Telekommunikationsdienst i. S. d. § 3 Nr. 17a Telekommunikationsgesetz (TKG) handelt, muss dieser die jeweils anwendbaren Vorgaben von DS-GVO und TKG erfüllen, hierunter insbesondere § 6 und Teil 7 TKG. Er ist im Hinblick auf die Einhaltung der telekommunikations- und datenschutzrechtlichen Anforderungen sorgfältig auszuwählen. Der Abschluss eines Vertrages gemäß Art. 28 Abs. 3 DS-GVO (s. u.) ist in diesem Fall entbehrlich.
2. Es muss gewährleistet sein, dass nur zugelassene Nutzer an einem Nachrichtenaustausch teilnehmen können. Dies gilt sowohl für die Kommunikation einer festgelegten, geschlossenen Benutzergruppe (z. B. Krankenhaus) als auch für die Kommunikation mit sonstigen Teilnehmern des Messenger-Dienstes. Hierfür bedarf es eines geeigneten Registrierungsprozesses oder entsprechender Autorisierungs-/Authentifizierungsmechanismen, etwa durch ein zentral administriertes Identitätsmanagementsystem.
3. Für die mit der Nutzung des Messenger-Dienstes verbundenen Verarbeitungstätigkeiten muss, sofern diese umfangreich sind, eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO durchgeführt

werden. Kommt eine von mehreren Verantwortlichen genutzte nichtöffentliche Plattform zum Einsatz, genügt es, eine DSFA einmalig für die Plattform durchzuführen.

4. Für die Messenger-Lösung ist durch das Krankenhaus eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zur Gewährleistung der Sicherheit der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen vorzunehmen (Art. 32 Abs. 1 lit. d DS-GVO).
5. Die Messenger-Lösung sollte einen Betrieb sowohl als Service eines Dienstleisters/Auftragsverarbeiters als auch in der technischen Infrastruktur des Krankenhauses erlauben (On-Premises).
6. Soweit für den Betrieb des Verfahrens auf Auftragsverarbeiter zurückgegriffen wird, muss sichergestellt sein, dass diese den Regelungen der Datenschutz-Grundverordnung unterfallen und die Anforderungen des Art. 9 Abs. 3 DS-GVO i. V. m. § 203 Abs. 3 StGB sowie weiterer ggf. relevanter Vorschriften (z. B. Krankenhausgesetze) erfüllen. Hierzu sollte auf Dienstleister in Deutschland, der Europäischen Union bzw. des europäischen Wirtschaftsraums zurückgegriffen werden.
7. Mit den insoweit eingebundenen Auftragsverarbeitern ist ein Vertrag nach Art. 28 Abs. 3 DS-GVO zu schließen. Mit Blick auf die hinreichenden Garantien technisch-organisatorischer Maßnahmen, der Verarbeitung im Einklang mit der DS-GVO sowie des Schutzes der Rechte der Betroffenen sollte der Dienstleister über entsprechende Nachweise verfügen (z. B. Zertifizierung nach Art. 42 DS-GVO, Zertifizierung nach European Privacy Seal, BSI-Grundschutz-Zertifizierung).
8. Für die bei dem Dienstleister im Rahmen der Messenger-Lösung gespeicherten Daten ist eine regelmäßige Löschung sicherzustellen (vgl. TZ. I.8). Personenbezogene Patientendaten müssen auf den Servern des Verantwortlichen gespeichert werden. Die temporäre Speicherfrist auf den Endgeräten soll daher so kurz wie möglich gehalten und in kurzen zyklischen Abständen vom Endgerät auf die vorgesehenen Server verlagert werden. Das gilt auch für eine etwaige Containerlösung in der Mobile-Messenger-App.
9. Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App zeitnah auf allen eingesetzten Geräten durchzuführen.

4. Kurzpapiere der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Kurzpapier Nr. 20

Einwilligung nach der DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als 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 dient als Zusammenfassung bzw. Ergänzung der Leitlinien zur Einwilligung des Europäischen Datenschutzausschusses (WP 259 rev.01 „Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679“).

Voraussetzungen und Unterschiede zu dem bis zum 24. Mai 2018 geltenden Recht

Auch unter Geltung der DS-GVO ist die Einwilligung eine zentrale Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Allgemeine Regelungen dazu lassen sich nunmehr nicht mehr dem Bundesdatenschutzgesetz (BDSG) entnehmen, sondern unmittelbar der DS-GVO (Art. 4 Nr. 11, Art. 7). Eine Einwilligung ist danach nur wirksam, wenn sie freiwillig und – bezogen auf einen bestimmten Fall – informiert abgegeben wird. Die Schriftform ist nicht erforderlich; ausreichend ist vielmehr eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung, durch die die betroffene Person ihr Einverständnis zur Datenverarbeitung unmissverständlich erteilt. Die bestätigende Handlung kann bei Vorliegen dieser Voraussetzungen auch elektronisch, durch „Anklicken“ eines Feldes im Internet, oder auch mündlich erfolgen. Bei der Wahl der geeigneten Form ist zu beachten, dass der Verantwortliche die Erteilung der Einwilligung nachweisen können muss (s. u.).

Aus Erwägungsgrund (ErwGr.) 32 der DS-GVO ist ersichtlich, dass Stillschweigen, bereits angeklickte Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen. Ebenso wenig gilt dies nach Auffassung des Europäischen Datenschutzausschusses für die einfache Weiternutzung eines Services. Für die Erteilung von Einwilligungen ist vielmehr ein aktives Verhalten der betroffenen Personen erforderlich. Anders als nach der bisher ergangenen Rechtsprechung (BGH, Urt. v. 16.07.2008, VIII ZR 348/06; BGH, Urt. v. 11.11.2009, VIII ZR 12/08) reicht es nun nicht mehr aus, die betroffenen Personen auf Vertragsklauseln zu verweisen, welche fiktiv erteilte Erklärungen

enthalten und bei denen es als wirksame Einwilligung gewertet wurde, wenn ein vorformulierter Einwilligungstext nicht durchgestrichen wurde oder ein Kreuz zur Nichterteilung einer Einwilligung nicht gesetzt wurde.

Besonderes Augenmerk ist nach der Datenschutz-Grundverordnung auf die Freiwilligkeit einer Einwilligung zu richten. Es kann nur dann davon ausgegangen werden, dass eine betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat, also in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (siehe ErwGr. 42). Dies ist beispielsweise in aller Regel nicht der Fall, wenn die Erfüllung eines Vertrages von einer Einwilligung in eine Datenverarbeitung abhängig gemacht wird, die für die Erfüllung des Vertrages nicht erforderlich ist (Art. 7 Abs. 4 i. V. m. ErwGr. 43 DS-GVO, sogenanntes Koppelungsverbot). Zudem liefert eine Einwilligung regelmäßig keine gültige Rechtsgrundlage, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und es deshalb unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde. Dies ergibt sich ebenfalls aus ErwGr. 43.

Die Einwilligung hat in informierter Weise zu erfolgen. In ErwGr. 42 der DS-GVO wird insbesondere darauf abgestellt, dass eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt wird, keine missverständlichen Klauseln enthalten sind und die betroffene Person mindestens darüber informiert wird, wer der Verantwortliche ist und zu welchen Zwecken ihre personenbezogenen Daten verarbeitet werden sollen. Darüber hinaus ist die betroffene Person nach Auffassung des Europäischen Datenschutzausschusses über die Art der verarbeiteten Daten, über ihr Recht, die Einwilligung jederzeit zu widerrufen, ggf. über die Verwendung der Daten für eine automatisierte Entscheidungsfindung und über mögliche Risiken von Datenübermittlungen in Drittländer ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Artikel 46 DS-GVO zu informieren.

Den Verantwortlichen trifft nach Art. 7 Abs. 1 DSGVO eine ausdrückliche Verpflichtung, die Erteilung der Einwilligung nachweisen zu können. Diese Verpflichtung steht mit der in Art. 5 Abs. 2 DS-GVO geregelten Rechenschaftspflicht im Zusammenhang. Dies gilt nicht nur im Sinne einer Beweislastregel, wenn das Vorliegen einer Einwilligung bestritten wird, sondern ganz allgemein. Auch bei Kontrollen der Aufsichtsbehörden muss daher der Nachweis über erteilte Einwilligungen erbracht werden können. Wird die Einwilligung elektronisch erteilt, so muss der Verantwortliche sicherstellen, dass die Einwilligung protokolliert wird. Nicht ausreichend ist es etwa, wenn lediglich auf die ordnungsgemäße Gestaltung der entsprechenden

Webseite verwiesen wird, ohne im Einzelfall den Nachweis der tatsächlich erteilten Einwilligung zu erbringen. Der Verantwortliche hat durch geeignete technische und organisatorische Maßnahmen dafür Sorge zu tragen, dass die Datenschutzgrundsätze, insbesondere die Rechenschaftspflicht, umgesetzt werden. Hierzu muss er technische Systeme einsetzen, die einen Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ermöglichen.

Die betroffene Person hat das Recht, die Einwilligung jederzeit zu widerrufen. Der Widerruf gilt mit Wirkung für die Zukunft. Auf die Einwilligung gestützte Verarbeitungsvorgänge in der Vergangenheit bleiben also rechtmäßig. Auf die Widerruflichkeit der Einwilligung muss der Verantwortliche vor Abgabe der Einwilligung hinweisen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung sein.

Fortgeltung von Einwilligungen

Vor Anwendbarkeit der DS-GVO erteilte Einwilligungen wirken nach ErwGr. 171 der DS-GVO fort, sofern sie der Art nach den Bedingungen der DSGVO entsprechen. Hierzu zählen insbesondere folgende Punkte:

– Die Erteilung einer wirksamen Einwilligung muss gem. Art. 7 Abs. 1 DS-GVO nachgewiesen werden können, was eine entsprechende Dokumentation voraussetzt.
– Die Einwilligung muss freiwillig abgegeben worden sein (Art. 4 Nr. 11 DS-GVO), wobei die besonderen Anforderungen nach Art. 7 Abs. 4 DSGVO i. V. m. ErwGr. 43 DS-GVO zu beachten sind.
– Erforderlich ist eine Willensbekundung für den bestimmten Fall, in informierter Weise und in unmissverständlicher Form (Art. 4 Nr. 11 DSGVO), wobei die Anforderungen nach Art. 7 Abs. 2 DSGVO i. V. m. ErwGr. 32 und 42 DS-GVO zu beachten sind.
– Der Verantwortliche muss Mechanismen bereithalten, die den Widerruf der Einwilligung ermöglichen und Informationen bereithalten, wie die Einwilligung widerrufen werden kann.
– Im Falle der Einwilligung durch ein Kind in Bezug auf Dienste der Informationsgesellschaft müssen die Voraussetzungen nach Art. 8 DS-GVO vorliegen.

Sind die obigen Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort. Die betroffene Person muss darüber hinaus zum Zeitpunkt der Abgabe der Einwilligungserklärung die Informationen zur Verfügung gehabt haben, die zur Abgabe einer informierten Einwilligung notwendig sind. Nach ErwGr. 43 sind dies mindestens Informationen darüber, wer der

Verantwortliche ist und für welche Zwecke die personenbezogenen Daten verarbeitet werden.

Diese Informationen sind zum Teil identisch mit den nach Art. 13 DS-GVO vorgesehenen Informationspflichten. Die darüber hinausgehenden Informationspflichten müssen für die Fortgeltung bisher erteilter Einwilligungen hingegen grundsätzlich nicht erfüllt worden sein. Unabhängig von den genannten Bedingungen für erteilte Einwilligungen müssen künftig die Informationspflichten nach Art. 13 DSGVO beachtet werden.

Folgen bei unwirksamer Einwilligung

Eine Einwilligung, die nicht den dargestellten Anforderungen genügt, ist unwirksam und kann nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden. Die Datenverarbeitung in diesem Fall auf eine andere Rechtsgrundlage zu stützen, beispielsweise die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DS-GVO), ist grundsätzlich unzulässig, denn der Verantwortliche muss die Grundsätze der Fairness und Transparenz (Art. 5 Abs. 1 lit. a DS-GVO) beachten. Jedenfalls ist ein willkürliches Wechseln zwischen Einwilligung und anderen Rechtsgrundlagen nicht möglich.

Erweist sich die Einwilligung als unwirksam oder kann der Verantwortliche das Vorliegen der Einwilligung nicht nachweisen, so ist die Verarbeitung der Daten auf dieser Grundlage rechtswidrig. Bei Verstößen gegen die Grundsätze der Verarbeitung, einschließlich der Bedingungen für die Einwilligung, kann von der zuständigen Aufsichtsbehörde nach Maßgabe von Art. 83 Abs. 5 lit. a DS-GVO eine Geldbuße verhängt werden. Außerdem kommen je nach den Umständen des Einzelfalls auch Schadensersatzansprüche der betroffenen Person in Betracht.

Besondere Kategorien von Daten und Einwilligung eines Kindes

Gemäß Art. 9 Abs. 2 lit. a DS-GVO ist für die Verarbeitung besonderer Kategorien von Daten (Gesundheitsdaten, genetische und biometrische Daten usw.) eine dafür ausdrückliche Einwilligung erforderlich; konkludente Handlungen sind also ausgeschlossen. Art. 8 DS-GVO enthält besondere Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft.

Besondere Verarbeitungssituationen

Auch für besondere Datenverarbeitungssituationen gibt es teilweise Sonderregelungen, die zu beachten sind. Im Beschäftigtendatenschutz sieht das neue BDSG gestützt auf die Öffnungsklausel des Art. 88 DS-GVO weiterhin das Erfordernis der Schriftform vor, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 26 Abs. 2 S. 3 BDSG; siehe dazu auch das Kurzpapier Nr. 14, zum Beschäftigtendatenschutz). Besonderheiten sind auch bei der Einwilligung in die Datenverarbeitung zu Forschungszwecken zu beachten.

Hinweis:
Anmerkung zur Nutzung dieses Kurzpapiers: Dieses Kurzpapier darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbstständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird: „Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0)“.

II
Zweiter Teil
2. Tätigkeitsbericht zur Informationsfreiheit

1. Einführung

Die Bedeutung der Informationsfreiheit ist in der Bevölkerung noch kaum wahrgenommen worden. Bei der Fülle der falschen und unvollständigen Informationen, die insbesondere in den sozialen Medien verbreitet werden, genügen Anforderungen an Seriosität der Presse und die rundfunkrechtliche Grundversorgung nicht mehr für die informationelle Daseinsvorsorge. Die informationelle Selbstbestimmung erfordert auch korrekte Informationen durch den Staat. Die Volkssouveränität und die Information über das Staatshandeln gehören untrennbar zusammen. Dieser Informationsanspruch darf nicht zu einem Abschöpfen staatlicher Informationen zu ausschließlich kommerziellen Zwecken verkommen. Der Beauftragte für Informationsfreiheit hat jeweils zu prüfen, ob ein Informationsbegehren der informationellen Selbstbestimmung dient.

Bezüglich der grundsätzlichen verfassungsrechtlichen Vorgaben und dogmatischen Grundlagen zum Hessischen Informationsfreiheitsgesetz verweise ich auf meine umfassenden Ausführungen in meinem ersten Tätigkeitsbericht zur Informationsfreiheit von 2018.

2. Informationsfreiheit bei hessischen Kommunen und Ministerien

Die Informationsfreiheit entwickelt sich gut in Hessen. Das zeigt sich bspw. auf der kommunalen Ebene, dasselbe gilt aber auch für den ministeriellen Bereich.

Kommunale Ebene

Bei hier eingegangenen Beschwerden, die sich gegen Kommunen richteten, fiel positiv auf, dass – anders als in den ersten Monaten nach Geltungsbeginn des Hessischen Informationsfreiheitsgesetzes, also des Vierten Teils des HDSIG (dessen §§ 80 ff. regeln die Informationsfreiheit) – die Kommunen, für die mangels eines entsprechenden Satzungsbeschlusses die Informationsfreiheit nicht gilt, die Ablehnung des Informationsantrages korrekt mit dem Hinweis auf § 81 Abs. 1 Nr. 7 HDSIG begründen, statt wie oft zu Beginn der hessischen Informationsfreiheit im Mai 2018 überhaupt nicht auf den Informationsantrag zu reagieren.

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für…

7. die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen ungeachtet ihrer Rechtsform, soweit die Anwendung des Vierten Teils durch Satzung ausdrücklich bestimmt wird.

Im Übrigen haben etwa die Stadt Kassel und die Landkreise Darmstadt-Dieburg sowie Groß-Gerau die Geltung des Informationsfreiheitsgesetzes beschlossen. Wahrscheinlich sind es noch mehr Kommunen, ohne dass mir dies bekannt ist. Für die entsprechenden Kommunen gibt es ja im Fall eines die Informationsfreiheit einführenden Satzungsbeschlusses keine dies betreffende Meldepflicht an das Innenministerium oder meine Behörde. In der Regel wird die Einführung über Medien bekannt oder kann insbesondere im Internet recherchiert werden.

Fall Darmstadt – Reichweite des Satzungsvorbehalts

Der gesetzlich angeordnete kommunale Satzungsvorbehalt für die Geltung der Informationsfreiheit (§ 81 Abs. 1 Nr. 7 HDSIG) unterstützt zwar die kommunale Selbstverwaltungsgarantie, der Vorbehalt bezieht sich aber

nicht nur auf Selbstverwaltungsaufgaben der Kommunen, sondern auch auf Weisungsaufgaben und Auftragsangelegenheiten.

Ein Bürger begehrte von der Stadt Darmstadt Auskunft über die Anzahl der von Privatpersonen angezeigten Verkehrsordnungswidrigkeiten sowie über die Anzahl der daraufhin geahndeten Verstöße für die Jahre 2017 und 2018. Die Stadt Darmstadt lehnte den Antrag ab und verwies zur Begründung darauf, dass sie keine die Anwendbarkeit des hessischen Informationsfreiheitsrechts bestimmende Satzung im Sinne von § 81 Abs. 1 Nr. 7 HDSIG beschlossen habe und schon deshalb kein Informationszugang eröffnet sei.

Daraufhin wandte sich der Betroffene an mich und trug vor, der Satzungsvorbehalt im Sinne von § 81 Abs. 1 Nr. 7 HDSIG beziehe sich nur auf kommunale Selbstverwaltungsaufgaben, er betreffe aber nicht die Konstellation wie hier, wenn nämlich der Oberbürgermeister keine kommunale Selbstverwaltungsaufgabe wahrnehme, sondern im Rahmen der Verkehrsüberwachung stattdessen Aufgaben zur Erfüllung nach Weisung/Auftragsangelegenheiten zu erledigen habe.

Rechtliche Bewertung

Zwar ist es zutreffend, dass das hessische Kommunalrecht zwischen Selbstverwaltungsaufgaben und solchen zur Erfüllung nach Weisung und Auftragsangelegenheiten unterscheidet. Die rechtlichen Einflussmöglichkeiten des Landes auf die Kommunen sind im Fall der Selbstverwaltung auf die Rechtsaufsicht beschränkt, während bei Weisungs- und Auftragsangelegenheiten fachaufsichtliche Einwirkungsmöglichkeiten bestehen, und zwar in Form von allgemeinen Weisungen und Weisungen für den Einzelfall (§§ 4, 135 Hessische Gemeindeordnung (HGO)).

Für die informationsfreiheitsrechtliche Frage des Zugangs zu amtlichen Unterlagen ist es in Hessen aber ohne Belang, welcher kommunale Aufgabenzweig betroffen ist. Denn der Wortlaut des § 81 Abs. 1 Nr. 7 HDSIG bezieht sich eindeutig auf kommunale Stellen als solche und differenziert gerade nicht danach, um welche Aufgabensparte es sich handelt.

Nicht nur der Wortlaut der Vorschrift sieht keine aufgabenbezogene Differenzierung vor, sondern auch die Begründung des Gesetzentwurfs gibt keinerlei Anlass, an dem stellenbezogenen Regelungscharakter des § 81 Abs. 1 Nr. 7 HDSIG zu zweifeln (vgl. Landtagsdrucks. 19/5728 S. 150 zu § 81).

Von daher unterfallen Bürgermeister und Oberbürgermeister auch dann der Regelung des § 81 Abs. 1 Nr. 7 HDSIG, wenn sie – etwa im Rahmen der örtlichen Verkehrsüberwachung – Aufgaben der örtlichen Ordnungsbehörden

und Kreisordnungsbehörden als Auftragsangelegenheit wahrnehmen (§ 4 Abs. 2 Satz. 1 HGO).

Etwas anderes gilt nur, wenn originär kommunale Organe organisationsrechtlich ausnahmsweise der Landesverwaltung zugeordnet werden, in diesem Kontext dann also nicht als kommunale Stelle handeln und insoweit auch nicht mehr dem kommunale Stellen betreffenden § 81 Abs. 1 Nr. 7 HDSIG unterfallen. Ein Beispiel findet sich im Bereich der Kommunalaufsicht, wenn der zur kommunalen Ebene gehörende Landrat speziell in seiner Funktion als Kommunalaufsichtsbehörde über die Gemeinden hier insoweit als Landesbehörde gesetzlich qualifiziert wird (§ 136 Abs. 3 HGO).

§ 136 HGO

…

(3) Aufsichtsbehörde der übrigen Gemeinden ist der Landrat als Behörde der Landesverwaltung.

Diese organisationsrechtliche Zuweisung des kommunalen Verwaltungsorgans Landrat zur Landesverwaltung im Kontext der Kommunalaufsicht wird aber gesetzlich gerade nicht vorgenommen, soweit es im Bereich der Verkehrsüberwachung um ordnungsbehördliche Tätigkeiten auf der Grundlage des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung geht (HSOG) geht. Das ergibt sich gerade aus § 85 HSOG, auf den der sich über die Auskunftsverweigerung beschwerende Bürger hingewiesen hatte.

§ 85 HSOG

(1) Allgemeine Ordnungsbehörde sind…

3. die Landräte in den Landkreisen und die Oberbürgermeister in kreisfreien Städten als Kreisordnungsbehörden…

Ich habe den Beschwerdeführer deshalb darüber unterrichtet, dass seine Ansicht, bei Weisungs- und Auftragsangelegenheiten sei der Satzungsvorbehalt des § 81 Abs. 1 Nr. 7 HDSIG nicht betroffen, weil die Ordnungsverwaltung (HSOG) keine Selbstverwaltungsaufgabe sei, unzutreffend ist. Denn auch in diesem Zusammenhang ist der Anwendungsbereich des § 81 Abs. 1 Nr. 7 HDSIG gegeben, soweit originär kommunale Behörden nicht ausnahmsweise der Landesverwaltung gesetzlich zugeordnet werden.

Ministerielle Ebene

Was die ministerielle Ebene betrifft, ist mir kein Fall bekannt, in dem entgegen meiner Beratung rechtswidrig kein Informationszugang gewährt wurde.

Kernbereich der Willens- und Entscheidungsbildung

Mitgetragen hatte ich die Entscheidung des Hessischen Innenministeriums im Jahr 2018, das den Gesetzgebungsprozess betreffend die Einführung der Informationsfreiheit vorbereitende/begleitende Evaluationsgutachten zur Informationsfreiheit in Bund und Ländern zunächst vom Informationszugang auszunehmen. Das Innenministerium hatte das damit begründet, dass die Bekanntgabe des Gutachtens den Kernbereich der Willens- und Entscheidungsbildung der Landesregierung betrifft (§ 84 Abs. 2 Nr. 1 HDSIG).

§ 84 HDSIG

(2) Der Antrag auf Informationszugang ist abzulehnen,

1. *wenn die Bekanntgabe der Information den Kernbereich der Willens- und Entscheidungsbildung der Landesregierung betrifft…*

Das hatte für einen gewissen Zeitraum die Versagung des Informationszugangs gerechtfertigt, der aber mittlerweile abgelaufen ist. Seit 2019 hat daher das Hessische Innenministerium Informationszugang in der Angelegenheit gewährt, was auch deshalb geboten ist, weil Gutachten grundsätzlich dem Informationszugang offenstehen (§ 84 Abs. 1HDSIG).

§ 84 Abs. 1 HDSIG

(1) Der Antrag auf Informationszugang kann abgelehnt werden für Entwürfe zu Entscheidungen sowie für Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung oder bevorstehender behördlicher Maßnahmen vereitelt würde. Nicht der unmittelbaren Entscheidungsvorbereitung nach Satz 1 dienen regelmäßig Ergebnisse der Beweiserhebung und Gutachten oder Stellungnahmen Dritter.

Fristen

Betreffend die ministerielle Ebene ist allerdings zu kritisieren, dass die für die Bearbeitung von Informationsanträgen geltenden Fristen nicht immer eingehalten werden und die für diese Konstellation vorgesehene Zwischennachricht oft ausbleibt.

§ 87 HDSIG

(1) Die informationspflichtige Stelle hat unverzüglich, spätestens innerhalb eines Monats, in den Fällen des § 86 spätestens innerhalb von drei Monaten nach Eingang des hinreichend bestimmten Antrags zu entscheiden. In den Fällen des § 86 ist die Entscheidung auch dem Dritten bekannt zu geben.

(…)

(4) Können die Informationen nicht oder nicht vollständig innerhalb der in Abs. 1 Satz 1 genannten Fristen zugänglich gemacht werden oder erfordern Umfang oder Komplexität eine intensive Prüfung, so kann die informationspflichtige Stelle die Frist um einen Monat verlängern. Die antragstellende Person ist über die Fristverlängerung unter Angabe der maßgeblichen Gründe schriftlich zu informieren.

Freilich fällt andererseits nicht positiv auf, dass antragstellende Personen, selbst wenn deren Anträge Drittbetroffenheit aufweisen und/oder bei denen sich die Frage stellen könnte, ob sie vielleicht wegen unverhältnismäßigen Verwaltungsaufwands im Sinne von § 85 Abs. 2 abgelehnt werden können, mitunter bei mir bereits Beschwerde einlegen, wenn ein Monat plus ein weiterer Tag ohne Informationszugang abgelaufen ist.

Art der Zugangsgewährung

Die Art der Zugangsgewährung ist in den §§ 80 ff. HDSIG nicht präzise geregelt.

Ein Beschwerdeführer rügte, dass das informationspflichtige Ministerium ihm zu einem Dokument nur durch Einsichtnahme vor Ort die Information gewähren wollte, statt ihm eine Kopie zu seinem Wohnsitz nach Berlin zu schicken, worum er gebeten hatte. Ich habe daraufhin das Ministerium darauf angesprochen, dem Beschwerdeführer die Anreise von Berlin nach Wiesbaden zu ersparen, und diesem Anliegen hat das Ministerium dann auch entsprochen.

Generell obliegt es der Entscheidung der informationspflichtigen Stelle zu bestimmen, in welcher Weise Informationszugang gewährt wird. Die §§ 80, 87 enthalten insoweit keine nähere Festlegung, und aus der Kostenregelung des § 88 ergibt sich nur, dass es verschiedene Arten der Informationsgewährung gibt.

§ 88 HDSIG

(1) Die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort sind nach dem Vierten Teil dieses Gesetzes kostenfrei…

In einem anderen Fall verwies das informationspflichtige Ministerium den Beschwerdeführer darauf, die vom Ministerium begehrte Information sei ja auch bei einer bestimmten Kommune vorhanden und deshalb solle/könne er sich die Information auch dort besorgen. Ich habe das Ministerium darauf hingewiesen, dass eine solche Vorgehensweise nicht zulässig ist, sondern die Stelle informationspflichtig ist, die über die begehrten Informationen verfügt. Das ergibt sich bereits deutlich aus der den Informationsantrag betreffenden Vorschrift § 85 HDSIG.

§ 85 HDSIG

(1) Ein Informationszugang wird auf Antrag bei der Stelle, die über die begehrten Informationen verfügt (informationspflichtige Stelle), gewährt.

Davon zu trennen ist umgekehrt der Aspekt, dass im Fall des Ausschlusses des Informationszuganges gegenüber bestimmten Stellen dieser Ausschluss nicht dadurch vereitelt werden kann, dass Informationen dieser Stellen noch zusätzlich bei anderen Stellen vorhanden sind, § 81 Abs. 3 HDSIG.

§ 81 HDSIG

(3) Soweit ein Informationszugang nach Abs. 1 oder 2 ausgeschlossen ist, gilt dies auch für Datei- und Aktenbestandteile, die sich in Dateien oder Akten anderer Behörden befinden.

3. Ordnungswidrigkeiten Flughafen Frankfurt (verspätete Landungen)

Gegenüber Behörden, die für Geldbußen zuständig sind, besteht insoweit kein Anspruch auf Informationszugang.

Ein Bürger begehrte beim Regierungspräsidium Darmstadt Zugang betreffend Unterlagen abgeschlossener Ordnungswidrigkeitenverfahren wegen verspäteter Landungen am Flughafen Frankfurt. Das zuständige Regierungspräsidium Darmstadt lehnte dies ab, weil das HDSIG durch das Ordnungswidrigkeitengesetz (OWiG) verdrängt werde und deshalb nicht anwendbar sei. Dies führte zur Beschwerde bei meiner Behörde.

Bewertung

Dem Regierungspräsidium Darmstadt ist insofern zuzustimmen, als das hessische Informationsfreiheitsrecht dann nicht anwendbar ist, soweit Auskunftsansprüche spezialgesetzlich geregelt sind. Diese Nachrangigkeit des hessischen Informationsfreiheitsrechts (dem Vierten Teil des HDSIG, nämlich die §§ 80 ff.) gegenüber speziellen Auskunftsansprüchen ist im HDSIG auch ausdrücklich normiert, § 80 Abs. 2 HDSIG.

> *§ 80 HDSIG*
>
> *(2) Soweit besondere Rechtsvorschriften die Auskunftserteilung regeln, gehen sie den Vorschriften des Vierten Teils vor.*

Jedoch enthält das Ordnungswidrigkeitengesetz keine Regelung über die Auskunft betreffend abgeschlossene Verfahren. Zudem zeigt auch das HDSIG mit Blick auf zwei Bestimmungen deutlich, dass es gerade auch Ordnungswidrigkeitenverfahren als Regelungsgegenstand hat. So soll zum einen durch das Informationszugangsrecht nicht bewirkt werden, dass der Ablauf von Ordnungswidrigkeitenverfahren beeinträchtigt wird. Unter der Beschreibung „Schutz besonderer öffentlicher Belange“ wird u. a. das Ordnungswidrigkeitenverfahren vor konkreten Nachteilen des Informationszugangs geschützt, § 82 Nr. 2. d) HDSIG.

§ 82 HDSIG

Ein Informationszugang besteht nicht…

2. bei Informationen, deren Bekanntwerden nachteilige Auswirkungen haben kann auf …

d) den Erfolg eines … Ordnungswidrigkeiten- oder Disziplinarverfahrens …

Bei abgeschlossenen Ordnungswidrigkeitenverfahren kann dieser Erfolg aber nicht mehr betroffen sein.

Neben dieser sachbezogenen Regelung gibt es aber weitere, und zwar stellenbezogene Regelungen, die eben diese Stellen, die für die Durchführung von Ordnungswidrigkeitenverfahren und damit für Geldbußen zuständig sind, vom Informationszugang ausnehmen, nämlich § 81 Abs. 1 Nr. 4 HDSIG mit Verweis auf die (den EU-Richtlinienbereich betreffenden) § 40 Abs. 2 i. V. m. § 40 Abs. 1 HDSIG. Und dieser Ausschluss gilt gerade auch für Behörden, die an sich keine Polizeibehörden sind, aber funktionell als Ordnungswidrigkeitenbehörde tätig werden (vgl. zum Ordnungswidrigkeitenverfahren auch Begründung des Gesetzentwurfs, Drucks. 19/5728, S. 136 zu § 40).

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für

…

4. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden und sonstige in § 40 Abs. 2 genannten Stellen sowie Disziplinarbehörden, jedoch nur, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, und nicht, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln.

§ 40 HDSIG

(1) Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten … zuständigen Stellen.

(2) Abs. 1 findet auch Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung und den Vollzug von Strafen … und von Geldbußen zuständig sind.

Den anfragenden Bürger habe ich deshalb darüber informiert, dass er gegenüber dem Regierungspräsidium Darmstadt mit Blick auf Verfahren betreffend die Verhängung von Geldbußen keinen Anspruch auf Informationszugang besitzt, hier also Akten zu abgeschlossenen Ordnungswidrigkeitenverfahren wegen verspäteter Landungen am Frankfurter Flughafen.

4. Das Gesetz zum Schutz von Geschäftsgeheimnissen

Das Gesetz zum Schutz von Geschäftsgeheimnissen lässt die Informationsfreiheit unberührt. Es definiert allerdings den Begriff „Geschäftsgeheimnis", der auch für den Informationszugang von Bedeutung ist.

Auf Bundesebene ist das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) vom 18.04.2019 in Kraft getreten. Es enthält auch Regelungen, die die Informationsfreiheit betreffen:

Wichtig ist zum einen die in § 1 Abs. 3 Nr. 2. GeschGehG getroffene Festlegung zum Anwendungsbereich des Gesetzes, wonach die Informationsfreiheit unberührt bleibt.

§ 1 GeschGehG

…

(3) Es bleiben unberührt: …

2. die Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit nach der Charta der Grundrechte der Europäischen Union (ABl. C 202 vom 7.6.2016, S. 389), einschließlich der Achtung der Freiheit und der Pluralität der Medien, …

Neben dieser Vorschrift sind zusätzlich die Regelungen in § 4 GeschGehG, der Handlungsverbote betrifft, und die in § 5 GeschGehG normierten Ausnahmen von den Handlungsverboten von Belang. Dadurch wird klargestellt, dass berechtigte Informationsfreiheitsanträge nicht von den Handlungsverboten des § 4 GeschGehG erfasst sind.

§ 5 GeschGehG

Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses fällt nicht unter die Verbote des § 4, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere

1. zur Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, einschließlich der Achtung der Freiheit und Pluralität der Medien …

Maßgebend ist das Gesetz zum Schutz von Geschäftsgeheimnissen nunmehr, soweit das Informationsfreiheitsrecht an den Rechtsbegriff Geschäftsgeheimnis anknüpft. So ist in § 82 Nr. 4 HDSIG geregelt, dass ein Anspruch auf Informationszugang nicht besteht bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat.

§ 82 HDSIG

Ein Anspruch auf Informationszugang besteht nicht…

4. bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat.

Was als Geschäftsgeheimnis zu gelten hat (der Terminus Betriebsgeheimnis ist im Geschäftsgeheimnisbegriff aufgegangen), regelt nunmehr § 2 GeschGehG.

§ 2 GeschGehG

Im Sinne dieses Gesetzes ist

1. Geschäftsgeheimnis eine Information

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht …

Es liegt auf der Hand, dass speziell die Regelung c) zu Debatten führen kann; bei den bisherigen Eingaben nach dem Informationsfreiheitsgesetz bei mir hat das Thema Geschäftsgeheimnis allerdings bislang noch keine größere Rolle gespielt.

ANHANG II

Materialien zur Informationsfreiheit

1. Entschließung der 37. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 12. Juni 2019 in Saarbrücken

Transparenz im Rahmen politischer Entscheidungsprozesse – Verpflichtendes Lobbyregister einführen

Die parlamentarische Demokratie lebt von der offenen und deshalb öffentlichen Diskussion verschiedener, oftmals unterschiedlicher Interessen, die im Rahmen der Gesetzgebung von den Parlamentsmitgliedern gegeneinander abgewogen werden müssen. Angesichts der Komplexität der sozialen und wirtschaftlichen Realität und der Regelungsmaterien kann es im demokratischen Willensbildungsprozess oftmals hilfreich sein, auf die Expertise von unterschiedlichen Personen, Gruppierungen und Beteiligten aus Gesellschaft und Wirtschaft zurückgreifen zu können. Die Art und Weise einer solchen Einflussnahme muss jedoch transparent sein. Die Bürgerinnen und Bürger sollen wissen, wer im Laufe des Entstehungsprozesses an der Formulierung eines Gesetzentwurfs beteiligt war und wer in wessen Auftrag und mit welchen Mitteln auf politische Entscheidungen einzuwirken versucht. Verflechtungen insbesondere zwischen Politik und Wirtschaft sind erkennbar zu machen, damit verdeckte Einflussnahmen erschwert sowie eine öffentliche Kontrolle ermöglicht wird.

Deshalb bestehen bereits in einigen Staaten Regelungen zur Führung von Lobbyregistern. Aus Sicht der Informationsfreiheitsbeauftragten in Deutschland ist es für ein demokratisches Gemeinwesen geboten, verpflichtend Register einzuführen, in die Informationen über Interessenvertretungen und deren Aktivitäten einzutragen sind. Darin sind mindestens die Namen der natürlichen und juristischen Personen unter Angabe ihrer Organisationsform, der Schwerpunkt der inhaltlichen oder beruflichen Tätigkeit und zumindest die wesentlichen Inhalte des Beitrags zum jeweiligen Gesetzgebungsverfahren zu veröffentlichen. Die damit hergestellte Transparenz stärkt das Vertrauen der Menschen in die Politik, ermöglicht demokratische Kontrolle und erhöht die Akzeptanz politischer – insbesondere gesetzgeberischer – Entscheidungen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Bundes- und die Landesgesetzgeber deshalb dazu auf, etwa in Anlehnung an das Thüringer Beteiligtentransparenzdokumentationsgesetz vom 7. Februar 2019 gesetzliche Rahmenbedingungen zur Einführung eines verpflichtenden Lobbyregisters zu verabschieden.

2. Positionspapier der 37. Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) am 12. Juni 2019 in Saarbrücken

Informationszugang in den Behörden erleichtern durch „Informationsfreiheit by Design“

Der digitale Wandel ist eine der großen Herausforderungen, vor denen die öffentliche Verwaltung heute steht. Gegenwärtig müssen E-Government-Gesetze sowie die Regelungen im Onlinezugangsgesetz umgesetzt werden. Parallel ist ein gestiegenes Interesse an der Transparenz des Verwaltungshandelns festzustellen, das die Gesetzgeber zunehmend aufgreifen. Die öffentliche Verwaltung ist in der Pflicht, das Recht auf Informationszugangsfreiheit umzusetzen. Das Vertrauen in die staatliche Aufgabenerfüllung wird gefestigt, indem Auskunftsersuchen schnell und effizient bearbeitet werden.

Vor diesem Hintergrund empfiehlt die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) den öffentlichen Stellen des Bundes und der Länder, die Anforderungen an die Informationsfreiheit bereits von Anfang an in die Gestaltung ihrer IT-Systeme und organisatorischen Prozesse einfließen zu lassen: „Informationsfreiheit by Design“. Die Gesetzgeber werden aufgerufen, die gesetzlichen Grundlagen zu schaffen und notwendige Ressourcen zur Verfügung zu stellen.

Definition

Zu „Informationsfreiheit by Design“ zählt die Gesamtheit technischer und organisatorischer Instrumente unter Berücksichtigung des Stands der Technik, die der Wahrnehmung und Erfüllung der Rechte nach den Informationsfreiheits- und Informationszugangsgesetzen, Umweltinformationsgesetzen und Transparenzgesetzen des Bundes und der Länder dienen. Damit unterstützt „Informationsfreiheit by Design“ einerseits informationspflichtige Stellen bei der Erfüllung eines beantragten Informationszugangs sowie bei der Umsetzung von Veröffentlichungspflichten, andererseits wird für Antragstellende der Informationszugang erleichtert.

Rahmenbedingungen

Für den Bereich der Verarbeitung personenbezogener Daten hat der europäische Verordnungsgeber das Prinzip des Datenschutzes durch Technikgestaltung – also „Datenschutz by Design“ – normiert. Auf dem Gebiet der Informationsfreiheit bestehen ebenfalls Regelungen, aus denen für informationspflichtige Stellen technische und organisatorische Verpflich-

tungen resultieren. Hierzu zählen je nach Regelungsinhalt der landes- und bundesrechtlichen Bestimmungen etwa

– proaktive Veröffentlichungspflichten,
– das Hinwirken auf eine Speicherung von Informationen in elektronischen Datenbanken,
– die Benennung von Ansprechpartnern oder anderen informationspflichtigen Stellen,
– die Bereitstellung von Verzeichnissen über verfügbare Informationen,
– die Einrichtung von öffentlich zugänglichen Informationsnetzen und -portalen,
– die Berücksichtigung der Kennzeichnung von Informationen durch Dritte als „schutzbedürftig“ und
– die Ermöglichung eines beschränkten Informationszugangs bei nur teilweise entgegenstehenden öffentlichen oder privaten Interessen.

Weiterhin soll die Beachtung der Grundsätze der ordnungsgemäßen Aktenführung dazu dienen, den zeitlichen Bereitstellungsaufwand zu begrenzen und die Kosten des Informationszugangs zu verringern.

Maßnahmen

Maßnahmen zu „Informationsfreiheit by Design“ können bei der Erfüllung dieser technischen und organisatorischen Verpflichtungen eine Hilfestellung bieten. So sollte die Auffindbarkeit von Informationen bei den informationspflichtigen Stellen z. B. durch effiziente Aktensystematik und elektronische Suchfunktionen gewährleistet sein. In Aktensystemen könnte bei Aufnahme neuer Informationen eine Kennzeichnung sensibler Abschnitte oder Aktenteile erfolgen, die eine gesonderte Prüfung auf geheimhaltungsbedürftige Teile erleichtert. Informationen sollten nach Möglichkeit in den Aktensystemen kategorisiert werden, was in bestimmten Verwaltungsbereichen etwa durch die Führung von Teilakten denkbar ist, die Teil einer Hauptakte sind. Veröffentlichungsfähige Informationen sollten durch die informationspflichtige Stelle proaktiv, etwa über ein Informationsportal, für die Allgemeinheit zur Verfügung gestellt werden.

Mit dem Ansatz „Informationsfreiheit by Design“ können standardisierte Lösungen für wiederkehrende Fragestellungen entwickelt werden, wodurch der Aufwand auf Verwaltungsseite reduziert wird. Diese Systemgestaltung obliegt dabei nicht nur den Verantwortlichen der öffentlichen Verwaltung, sondern auch den Entwicklerinnen und Entwicklern von Software-Lösungen für öffentliche Verwaltungen, bei denen Anforderungen der Informationsfreiheit von Anfang an in die Konzepte und Implementierungen aufgenommen werden sollten.

Sachwortverzeichnis