Neunundvierzigster Tätigkeitsbericht zum Datenschutz
und
Dritter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Michael Ronellenfitsch

vorgelegt zum 31. Dezember 2020
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

49. Tätigkeitsbericht zum Datenschutz / 3. 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 zu I

Verzeichnis der Abkürzungen

ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
AG	Aktiengesellschaft
AO	Abgabenordnung
Art.	Artikel
AsylbLG	Asylbewerberleistungsgesetz
BAG	Bundesarbeitsgericht
BBB	BigBlueButton
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDSG	Bundesdatenschutzgesetz
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung
Beschl.	Beschluss
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BTDrucks., BT-Drs.	Bundestagsdrucksache
BTLE	Borders, Travel & Law Enforcement (Subgroup)
BVerfG	Bundesverfassungsgericht
bzw.	beziehungsweise
ca.	circa
COVID-19	Coronavirus-Krankheit-2019
CSC	Coordinated Supervision Committee
d. h.	das heißt
DIN	Deutsche Industrie-Norm(en)
DSO	Deutsche Stiftung Organtransplantation
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; kurz: Datenschutzkonferenz
e. V.	eingetragener Verein
EDSA	Europäischer Datenschutzausschuss

EN	European Norm
ERVV	Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere Behördenpostfach
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
Eurodac SCG	Eurodac Supervision Coordination Group
f.	folgende
ff.	folgende (Seiten) / fortfolgende
GDPR	General Data Protection Regulation (= DS-GVO)
ggf.	gegebenenfalls
GVBl.	Gesetz- und Verordnungsblatt (Hessen)
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HGO	Hessische Gemeindeordnung
HKM	Hessisches Kultusministerium
HSÜG	Hessische Sicherheitsüberprüfungsgesetz
HSÜVG	Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz
i. d. R.	in der Regel
IEC	International Electrotechnical Commission
INA	Innenausschuss
i. R. d.	im Rahmen der/des
i. S. d.	im Sinne der/des
ISO	International Organization for Standardization (Internationale Normierungsorganisation)
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IfSG	Infektionsschutzgesetz
IKU	Inkassounternehmen
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
IT	Informationstechnik

Kfz	Kraftfahrzeug
KOM	Europäische Kommission
LDA	Landesamt für Datenschutzaufsicht
lit.	Littera
LAG	Landesarbeitsgericht
lsbh	Landessportbund Hessen
LT-Drs.	Landtagsdrucksache (Hessen)
LUSD	Lehrer- und Schülerdatenbank
MTA	Mail Transfer Agent
MUA	Mail User Agent
ND	Namensdienst
Nr.	Nummer
OFD	Oberfinanzdirektion
o. g.	oben genannt/genannte/genannter/genanntes
OwiG	Gesetz über Ordnungswidrigkeiten
QR-Code	Quick Response Code
Rdnr./Rn.	Randnummer
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
s. a.	siehe auch
SDM	Standard-Datenschutzmodell
SIS II SCG	Schengen Information System II Supervision Coordination Group
sog.	sogenannte/sogenannter/sogenanntes
SSA	Staatliches Schulamt
StGB	Strafgesetzbuch
StBerG	Steuerberatungsgesetz
TB	Tätigkeitsbericht
u. a.	unter anderem
UK	United Kingdom (Vereinigtes Königreich)
US(A)	Vereinigte Staaten von Amerika

usw.	und so weiter
v.	von
vgl.	vergleiche
VIS SCG	Visa Information System Supervision Coordination Group
VKS	Video-Konferenzsystem
WHO	World Health Organization (Weltgesundheits-organisation)
WLAN	Wireless Local Area Network
z. B.	zum Beispiel
Ziff.	Ziffer

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
Asylbewerber-leistungsgesetz	Asylbewerberleistungsgesetz in der Fassung der Bekanntmachung vom August 1997 (BGBl. I S. 2022), zuletzt geändert durch Gesetz vom 21. Dezember 2020
AO	Abgabenordnung 1.10. 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Artikel 28 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3096)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019 (BGBl. I S. 1626)
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)
12. BImSchV	Störfall-Verordnung in der Fassung der Bekanntmachung vom 15. März 2017 (BGBl. I S. 483), die zuletzt durch Artikel 107 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert wurde
CoKoBeV/Corona-Kontakt- und Betriebs Beschränkungs-verordnung	Verordnung zur Beschränkung von sozialen Kontakten und des Betriebes von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie (Corona-Kontakt- und Betriebsbeschränkungsverordnung) vom 7. Mai 2020, aufgeh. durch Artikel 4 Nr. 3 der Verordnung vom 26. November 2020 (GVBl. S. 826)
CoKoBeV/Corona-Kontakt- und Betriebs-beschränkungs-verordnung	Verordnung zur Beschränkung von sozialen Kontakten und des Betriebes von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie in der Fassung der am 15. August 2020 in Kraft tretenden Änderungen durch Art. 3 der Siebzehnten Verordnung zur Anpassung der Verordnungen zur Bekämpfung des Corona-Virus vom 11. August 2020 (GVBl. S. 538)
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)

GenG	Genossenschaftsgesetz i. d. F. vom 16.10.2006 (BGBl. I S. 2230), zuletzt geändert durch Gesetz vom 22.12.2020 (BGBl. I S. 3256)
GWG	Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch Artikel 269 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328)
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)
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)
HSchG	Hessisches Schulgesetz vom 01.08.2017, zuletzt geändert durch Art. 1 des Gesetzes vom 29,09.2020 (GVBl. S. 706).
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung vom 14.01.2005 (GVBl. I 2005 S. 14), zuletzt geändert durch Artikel 19 Hess. Ausländer-TeilhabeG vom 07.05.2020 (GVBl. S. 318)
HSÜG	Hessische Sicherheitsüberprüfungsgesetz vom 19.12.2014, Überschrift neu gefasst und geändert durch Gesetz vom 11.12.2019 (GVBl. S. 406)
HSÜVG	Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz (HSÜVG) vom 19.12.2014, geändert durch Gesetz vom 11.12.2019 (GVBl. S. 406)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen vom 20.07.2000 (BGBl. I S. 1045), zuletzt geändert durch Artikel 4a des Gesetzes vom 21.12.2020 (BGBl. I S. 3136)
KAG	Gesetz über kommunale Abgaben in der Fassung vom 24.03.2013 (GVBl.2013, 134) zuletzt geändert durch Art. 1 Gesetz zur Neuregelung der Erhebung von Straßenbeiträgen vom 28.05.2018 (GVBl. S. 247)
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Artikel 4 des Gesetzes vom 09.12.2020 (BGBl. I S. 2773)

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
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 3 des Gesetzes vom 30.11.2020 (BGBl. I S. 2600)
PAuswG	Personalausweisgesetz vom 18.06.2009 (BGBl. I S. 1346), zuletzt geändert durch Artikel 13 des Gesetzes vom 03.12.2020 (BGBl. I S. 2744)
SGB I	Das Erste Buch Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11.12.1975, BGBl. I S. 3015), zuletzt geändert durch Gesetz vom 12.06.2020 (BGBl. I S. 1248, 1255)
SGB X	Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz, in der Fassung der Bekanntmachung vom 18.01.2001 (BGBl. I S. 130), zuletzt geändert durch Gesetz vom 03.12.2020 (BGBl. I S. 2668, 2673)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 47 des Gesetzes vom 21.12.2020 (BGBl. I S. 3096) geändert worden ist
StBerG	Steuerberatungsgesetz in der Fassung der Bekanntmachung vom 04.11.1975 (BGBl. I S. 2735), zuletzt geändert durch Artikel 37 des Gesetzes vom 21.12.2020 (BGBl. I S. 3096)
StVG	Straßenverkehrsgesetz vom 05.03 2003, zuletzt geändert durch Art. 3 des Gesetzes vom 26.11.2020 (BGBl. I S. 2575)
TPG	Gesetz über die Spende, Entnahme und Übertragung von Organen und Geweben vom 04.09.2007 (BGBl. I S. 2206, TPG), zuletzt geändert durch Art. 6 Patientendaten-Schutz-G vom 14.10.2020 (BGBl. I S. 2115)

Kernpunkte

1. Anzahl und Prüfungsaufwand der Verfahren in europäischer Zusammenarbeit (Kohärenz-, Kooperations-, BCR-Verfahren) mit Beteiligung des HBDI nehmen ständig zu und intensivieren sich. Nicht zuletzt durch den Brexit und das sog. Schrems II-Urteils des EuGHs sind massive datenschutzrechtliche Auswirkungen auch im Drittlanddatenverkehr zu erwarten (Teil I Ziff. 2.1 und 2.2).
2. Die Umsetzung der Corona-Schutzmaßnahmen führten in vielen alltäglichen Lebensbereichen zu datenschutzrechtlichen Beschwerden, Nachfragen und Beratungen von Betroffenen und für die Datenverarbeitung Verantwortlichen. Dies betraf z. B. Schulen (Teil I Ziff. 5.1, 5.2), Kommunen (Teil I Ziff. 3.1), Unternehmen (Teil I Ziff. 8.3), Krankenhäuser (Teil I Ziff. 8.1), Sportvereine (Teil I Ziff. 10.1), Gaststätten (Teil I Ziff. 11.6), Friseurbetriebe (Teil I Ziff. 11.6), den Einsatz von Werbemaßnahmen (Teil I Ziff. 13.2) und E-Mails (Teil I Ziff. 14.1).
   Vermutlich war der vermehrte, Corona-bedingte (Zwangs-)Aufenthalt vieler Menschen in ihrem Zuhause ein Grund dafür, dass auch die Eingaben zur Videoüberwachung im nachbarlichen Kontext wieder vermehrt anstiegen (Teil I Ziff. 9.1).
3. Nach wie vor war ein zentraler Schwerpunkt die Bearbeitung von Beschwerden, Nachfragen und Beratungen zur Ausübung von Betroffenenrechten, wie dem Recht auf Löschung 17 DS-GVO (Teil I Ziff. 3.2; 11.2, 12.2, 12.3) oder dem Recht auf Auskunft 15 DS-GVO (Teil I Ziff. 6.3, 12.1,12.2, 12.3) sowie zur Einwilligung (Teil I Ziff. 7.1, 7.2, 7.3, 12.3) und deren Widerruf (Teil I Ziff. 7.1), zur Zugangskontrolle (Teil I Ziff. 11.4) und zu den Informationspflichten nach Art. 14 DS-GVO (Teil I Ziff. 12.2).
4. Mit der Novellierung des Hessischen Sicherheitsüberprüfungsgesetzes, jetzt Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz, wurden datenschutzrechtliche Sonderregelungen geschaffen und Untersuchungsbefugnisse des HBDI eingeschränkt (Teil I Ziff. 4.1).
5. Meldungen von Datenschutzpannen und Datenschutzverletzungen gemäß Art. 33 DS-GVO bilden mittlerweile einen Großteil der reaktiven Tätigkeit meiner Aufsichtsbehörde (Teil I Ziff. 6.1, 8.4, 8.7, 15.1, 15.2, 17.2). So führte Corona-bedingtes Arbeiten im Home-Office zu weiteren Vorfällen in neuen Konstellationen, wie z. B. unzulässige Datenoffenbarungen bei der Nutzung von Videokonferenzsystemen oder privater Endgeräte im Homeoffice (Teil I Ziff. 15.1).

6. Auch die Verarbeitungen personenbezogener Daten durch Banken und Kreditinstitute sind nur zulässig, wenn eine entsprechende Rechtsgrundlage diese vorsieht. Diese finden sich oft auch im Zivilrecht (Teil I Ziff. 11.1), bisweilen kann das Vorliegen eines berechtigten Interesses seitens des Kreditinstitutes Voraussetzung sein. Wird dabei das Vorliegen eines berechtigten Interesses zur Zulässigkeitsvoraussetzung erklärt, ist das Schwärzen von Daten auf vorzulegenden Dokumenten in der Regel zulässig (Teil I Ziff. 11.3).
7. Die gemeinsame länderübergreifende Prüfung von Trackingverfahren (Einsatz von Cookies) bei Zeitungs-Webseiten hat begonnen und soll langfristig eine rechtskonforme Praxis sicherstellen (Teil I Ziff. 13.1).
8. Schwerpunkte im Bereich der Sanktionen und Bußgeldverfahren waren wiederholte Verstöße gegen Betroffenenrechte und die sogenannten Mitarbeiterexzesse. Hinzu kamen Corona-bedingte Sachverhalte (Teil I Ziff. 6.1, 16.2).
9. Der Konzeption des Hessischen Informationsfreiheitsgesetzes würde es entsprechen, wenn der Gesetzgeber den Informationszugang auch gegenüber dem Landesamt für Verfassungsschutz und der Polizei angemessen eröffnen würde (Teil II.2).
10. Eingaben in der Zuständigkeit des Hessischen Informationsfreiheitsbeauftragten sind nur leicht gestiegen (Teil II.5, 6).

Vorwort

Während der Bearbeitung dieses Tätigkeitsberichts wechselte der Amtsinhaber des Hessischen Beauftragten für Datenschutz- und Informationsfreiheit. Auch wenn durch die Gesetzesbindung der Amtsinhaber die Kontinuität der Amtsführung gewährleistet ist, besteht insoweit keine Gesamtrechtsnachfolge. Die Formulierung der Datenschutzpolitik der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit ist vielmehr eine autonome Angelegenheit der Person, die jeweils das Amt innehat. Der 49. Tätigkeitsbericht betrifft einen Zeitraum, in dem der frühere Datenschutzbeauftragte zuständig war. Daraus folgt, dass dieser grundsätzlich auch die sachliche Verantwortung für den 49. Tätigkeitsbericht trägt. Die formelle Letztentscheidung und -verantwortung für den Tätigkeitsbericht obliegt demgegenüber dem gegenwärtigen Amtsinhaber. Dem entspricht die Gliederung dieses Tätigkeitsberichts. Der frühere Amtsinhaber berichtet über den Zeitraum seiner Verantwortlichkeit. Der gegenwärtige Amtsinhaber führt demgegenüber in die aktuelle Situation des Datenschutzes und die zu erwartende Entwicklung des Datenschutzrechts ein.

Abgesehen von dieser Unterscheidung folgt die Gliederung dieses Berichts der Gliederung der bisherigen Berichte.

Prof. Dr. Michael Ronellenfitsch

Zur Revitalisierung des Datenschutzes nach Abklingen der Pandemie

Anmerkungen des neuen HBDI Prof. Dr. Alexander Roßnagel

Seit dem 1.3.2021 übe ich das Amt des Hessischen Beauftragten für Datenschutz und Informationsfreiheit aus. Insofern liegt die Verantwortung für den Zeitraum, den der vorliegende 49. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten und der 3. Tätigkeitsbericht des Hessischen Beauftragten für Informationsfreiheit abdeckt, beim bisherigen Amtsinhaber Prof. Dr. Michael Ronellenfitsch. Da beide Berichte aber in meiner Amtszeit veröffentlicht werden, möchte ich für diese Berichte einige – eher zukunftsgerichtete – Überlegungen zu den Aufgaben und zur Organisationsentwicklung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit festhalten.

Der Schutz der Grundrechte der von Datenverarbeitung betroffenen Personen hat an Bedeutung und Aufmerksamkeit gewonnen. Seine Bedeutung steigt, weil die Digitalisierung zu einer intensiveren Verarbeitung personenbezogener Daten führt. Größere Aufmerksamkeit erfährt der Datenschutz, weil das europäische Datenschutzrecht neue Pflichten der Verantwortlichen und erweiterte Rechte der betroffenen Personen auch mit wirksamen Handlungs- und Sanktionsmöglichkeiten der Datenschutzaufsicht verbindet.

Dennoch wird die Umsetzung von Datenschutz immer schwieriger und verursacht neue Herausforderungen für die Hessische Datenschutzaufsicht. Hierfür ursächlich sind vor allem die folgenden Entwicklungen:

Zum einen nehmen die Risiken für die Grundrechte auf Datenschutz und informationelle Selbstbestimmung qualitativ und quantitativ zu. Die digitale Erfassung des alltäglichen Lebens durch das Internet der Dinge (z. B. durch vernetzte Automobile, Smart Meter, Smart Home und Smart Offices, Sprachassistenten, Gesundheits-Apps) erzeugt und erfordert zusätzliche Daten. Virtuelle Infrastrukturen (z. B. Suchsysteme, Social Media, Cloud Computing und Austauschplattformen) ermöglichen digitale Handlungsfähigkeit, zugleich aber auch die Bildung intensiver Persönlichkeitsprofile. Neue Methoden, personenbezogene Daten auszuwerten (Big Data, Künstliche Intelligenz), ermöglichen neue Erkenntnisse und Schlussfolgerungen, aber auch neue Möglichkeiten der Verhaltenssteuerung. Die mit Digitalisierung verbundenen Chancen zu nutzen und Risiken zu vermeiden, erfordert eine datenschutzgerechte Gestaltung solcher Informationstechnik-Systeme. Dies gilt sowohl für Unternehmen – insbesondere wenn sie datengetriebene Geschäftsmodelle verfolgen. Dies gilt aber ebenso für die Verwaltung – soweit

sie Digitalisierung für die zusätzliche Sammlung von Daten über Bürgerinnen und Bürger nutzt.

Zum anderen verursacht die Digitalisierung für die Verantwortlichen zusätzliche Pflichten, bringt zusätzliche Anforderungen mit sich und erfordert zusätzliche Aufmerksamkeit. Damit kommen große Unternehmen und Verwaltungen einigermaßen zurecht. Dies kann kleine und mittlere Unternehmen aber leicht überfordern. Das Einfordern der Datenschutzpflichten darf aber im Ergebnis nicht zu einer Reduzierung des Datenschutzes führen. Vielmehr müssen datenschutzgerechte Lösungen gefunden werden, die auch Datenschutz in kleinen und mittleren Unternehmen und in kleinen Gemeinden gewährleisten.

Drittens bringt die weltweite Vernetzung neue Herausforderungen mit sich, wenn sie nicht zu einer Reduzierung des Datenschutzes führen soll. Hier gibt der Europäische Gerichtshof den Datenschutzaufsichtsbehörden neue Aufgaben. Nach seiner Rechtsprechung muss jeder Verantwortliche, der personenbezogene Daten in Staaten außerhalb des Europäischen Wirtschaftsraums übermittelt, sicherstellen, dass dort der Grundrechtsschutz bezogen auf die personenbezogenen Daten in vergleichbarer Weise gewährleistet wird. Diese Anforderung ist für die Übermittlung in viele Staaten ein Problem. Für die USA hat der Gerichtshof ausdrücklich festgestellt, dass wegen der unbegrenzten Zugriffsmöglichkeit der Sicherheitsbehörden und Nachrichtendienste sowie wegen des fehlenden Rechtsschutzes für betroffene Personen aus Europa dort kein vergleichbares Datenschutzniveau besteht. Damit entsteht die neue Herausforderung, Übermittlungen von Daten in die USA zu unterbinden. Indirekt hat der Gerichtshof das Ziel vorgegeben, die bestehende Abhängigkeit von Anbietern aus USA zu reduzieren und in der Union eine möglichst weitgehende digitale Souveränität zu erreichen: Verantwortliche dürfen nur noch Informationstechnik einsetzen, die ihnen ermöglicht, die datenschutzrechtlichen Anforderungen zu erfüllen. Ohne Unternehmen und Behörden arbeitsunfähig zu machen, kann dies aber nur erreicht werden, wenn im Binnenmarkt funktionaläquivalente Alternativen zu den Informationstechnik-Systemen aus USA angeboten werden.

Schließlich hat die Corona-Pandemie die Umsetzung von datenschutzrechtlichen Anforderungen erschwert. Sie zwang und zwingt zu sozialer Distanz. Und sie zwang und zwingt zu Maßnahmen der Digitalisierung (wie Homeoffice, Videokonferenzen, elektronischer Aktenbearbeitung und anderen elektronischen Kommunikationsformen), um dennoch das gesellschaftliche Leben, den wirtschaftlichen Austausch und die öffentliche Verwaltung aufrecht zu erhalten. Aufgrund der extrem kurzen Reaktionszeit auf den ersten Lockdown im Frühjahr 2020 haben viele Organisationen, Unternehmen und Verwaltungen, Hochschulen und Schulen auf verfügbare und funktionsfähige

digitale Lösungen zurückgegriffen – ohne dabei auf Datenschutz zu achten. Der Datenschutz hat dadurch erheblich und auf breiter Front zurückgesteckt. Dennoch haben die Aufsichtsbehörden diese Lösungen aufgrund der gesellschaftlichen Notsituation vorübergehend geduldet. Wenn die Corona-Pandemie überwunden ist und wieder normale gesellschaftliche Verhältnisse herrschen, werden diese digitalen Lösungen zwar an Bedeutung verlieren, aber nicht verschwinden, weil sie ihre Tauglichkeit weitgehend bewiesen haben. Dann aber wird es auch notwendig sein, alle gefundenen Lösungen auf den Prüfstand zu stellen und an die datenschutzrechtlichen Anforderungen anzupassen.

Diesen Herausforderungen muss sich die hessische Datenschutzaufsicht in den kommenden Jahren stellen. Sie hofft dafür auf das Verständnis und sogar die Unterstützung durch die öffentlichen und nicht öffentlichen Stellen in Hessen. Denn: Private Angebote und öffentliche Aufgabenerfüllung sind auf Vertrauen angewiesen. Dies ist nur zu erreichen durch eine datenschutzgerechte Digitalisierung. Daher ist es notwendig, in der Entwicklung von Informationstechnik-Projekten möglichst frühzeitig eine datenschutzgerechte Gestaltung anzustreben und bei (coronabedingten) Fehlentwicklungen nach konstruktiven Korrekturen zu suchen.

Um diese Herausforderungen bewältigen zu können, ist für die Aufsichtsbehörde in Hessen ein geeigneter Handlungsrahmen notwendig. Dieser wird vor allem durch die Europäisierung des Datenschutzes bestimmt. Der europäische Rechtsrahmen bietet grundsätzlich hilfreiche Grundlagen und Instrumente. Um sie richtig nutzen zu können, sind aber organisatorische Anpassungen in der Datenschutzaufsicht erforderlich:

Um einen einheitlichen Vollzug des Datenschutzes in der Union sicherzustellen, sieht die Datenschutz-Grundverordnung (DS-GVO) eine enge grenzüberschreitende Zusammenarbeit der Aufsichtsbehörden in den Mitgliedstaaten vor. Berührt ein Aufsichtsverfahren mehrere Mitgliedstaaten, sollen sich die Aufsichtsbehörden über die erforderlichen Maßnahmen einigen. Kommt keine Einigung zustande, entscheidet der Europäische Datenschutzausschuss in dem umstrittenen Aufsichtsverfahren abschließend. Er besteht aus den Datenschutzbeauftragten der Mitgliedstaaten. Der Ausschuss ist außerdem unabhängig von einzelnen Aufsichtsverfahren zuständig, unionsweit festzulegen, wie die abstrakten Vorschriften der DS-GVO im Praxisvollzug zu verstehen sind. Wer darauf einwirken will, wie der Datenschutz in der Union künftig verstanden und praktiziert wird, muss sich aktiv in die Zusammenarbeit der Aufsichtsbehörden und in die Arbeit des Europäischen Datenschutzausschusses einbringen. Hierfür hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit eine Stabsstelle eingerichtet. Diese muss

allerdings den steigenden Arbeitserfordernissen entsprechend weiter ausgebaut werden, wenn sie ihr Ziel erreichen soll.

Eine zweite Stabsstelle wurde ebenfalls in Reaktion auf die veränderten Vollzugsbedingungen des Datenschutzes eingerichtet. Sie betrifft das Justiziariat. Die DS-GVO hat die Aufgaben und Handlungsmöglichkeiten der Aufsichtsbehörde ausgeweitet. Vor allem kann sie zur Durchsetzung von Datenschutzrecht gegenüber nicht öffentlichen Verantwortlichen Anordnungen zur Datenverarbeitung treffen und bei Verstoß gegen Datenschutzvorschriften empfindliche Sanktionen (Bußgelder) verhängen. Anordnungen und Bußgelder führen jedoch zu gerichtlichen Streitverfahren. Von beiden Instrumenten kann also sinnvoll nur Gebrauch gemacht werden, wenn die Aufsichtsbehörde auch in der Lage ist, die sich anschließenden Gerichtsprozesse erfolgreich durchzuführen. Das Justiziariat unterstützt die Fachreferate beim Erlass von Anordnungen und Verwarnungen, erlässt selbst die Bußgeldbescheide und betreut die gerichtlichen Verfahren. Aus diesem Grund ist auch diese Stabsstelle so auszubauen, dass eine „Waffengleichheit“ mit den Anwaltskanzleien der betroffenen Unternehmen besteht.

Für die Wahrnehmung der Grundrechte und die Teilnahme an der demokratischen Willensbildung ist in einer digitalen Gesellschaft neben dem Datenschutz der Zugang zu öffentlichen Informationen von besonderer Bedeutung. Diese Informationsfreiheit ist in Hessen erst seit 2018 im Gesetz vorgesehen. Ihre praktische Inanspruchnahme und Erfüllung müssen sich in Hessen erst noch entwickeln. Der Informationszugang ist im Gesetz für die Landesverwaltung vorgesehen, für die Gemeinden und Landkreise aber nur, wenn sie die Anwendung des Anspruchs auf Informationszugang für ihre öffentlichen Stellen durch Satzung ausdrücklich festgelegt haben. Dies haben bisher nur wenige Gemeinden und Landkreise beschlossen. Hier werden in den nächsten Jahren weitere Diskussionen zu den Vor- und Nachteilen eines Informationsanspruchs zu führen sein. Für den Hessischen Beauftragten für Informationsfreiheit ist die weitere Entwicklung und Durchsetzung des Informationszugangs zu öffentlichen Stellen eine wichtige Aufgabe.

Abschließend möchte ich mich bei meinem Vorgänger, Prof. Dr. Michael Ronellenfitsch, sehr herzlich dafür bedanken, dass er mir ein so wohl geordnetes Haus übergeben und mir durch Vorkehrungen und Ratschläge die Übernahme des Amts sehr erleichtert hat, vor allem aber auch dafür, dass er noch die Erstellung des Berichts über das letzte Jahr seiner Amtsführung übernommen hat und ihn hiermit vorlegt.

Prof. Dr. Alexander Roßnagel

I
Erster Teil
49. Tätigkeitsbericht zum Datenschutz

1. Einführung Datenschutz

Im Vorwort wurde darauf hingewiesen, dass bei der Neuwahl der oder des Datenschutzbeauftragten dessen oder deren Amtsdauer und die Geltungsdauer des Tätigkeitsberichts asynchron sind. Der Abgabezeitpunkt des Berichts bezeichnet nur den Berichtsgegenstand. Datenschutzrechtlich relevantes Ereignis (Verstoß und Reaktion) und Bericht über dieses Ereignis fallen ohnehin nicht zusammen. Beim Amtswechsel vergrößert sich diese Zeitspanne noch. Die datenschutzrechtlich relevanten Vorgänge, die im Tätigkeitsbericht zu behandeln sind, verlieren dadurch vollends ihren Nachrichtenwert und verleihen dem Tätigkeitsbericht generellen Bilanzcharakter.

Aufgabe des Tätigkeitsberichts ist es damit nicht allein, Datenschutzverstöße zu offenbaren und eine parlamentarische Kontrolle der Aufsichtsbehörden zu ermöglichen, sondern umgekehrt auch auf Ausstattungsmängel hinzuweisen, die sie an einer effektiven Aufgabenerfüllung hindern (vgl. Art. 52 Abs. 4 DS-GVO). Ein Ausstattungsmangel besteht meines Erachtens unter dem Gesichtspunkt der Waffengleichheit mit den zu Kontrollierenden. Da im privaten Bereich als Reaktion auf unsere Eingriffsbefugnisse juristisch-personell aufgerüstet wurde, ist es unabdingbar, dass die Aufgaben der Stabsstelle Justiziariat von Personal in der angemessenen Hierarchieebene wahrgenommen werden. So sollte eine Anhebung der Leitung des Justiziariats vorgenommen werden. Entsprechendes gilt für den europäischen Bereich. Hier muss die Bedeutung der europäischen Fragestellungen auch durch einen angemessenen Status der Repräsentantin oder des Repräsentanten meiner Behörde auf europäischer und internationaler Ebene sichergestellt werden. Im europäischen und internationalen Bereich lässt sich dies erreichen, durch die Kombination mit meiner Stellvertretung, die zur Eingruppierung nach B 4 (Anlage I HBesG) führt. Folgerichtig muss auch die Eingruppierung in der Stabsstelle Justiziariat angemessen (mind. B 3) erfolgen.

Im Übrigen wurde die Tätigkeit meiner Behörde maßgeblich durch die Corona-Pandemie beeinflusst. Hier galt es zu verhindern, dass vollendete Tatsachen für die Zeit nach dem Abklingen der Pandemie geschaffen werden. Dies setzte die Funktionsfähigkeit meiner Behörde voraus. Die Funktionsfähigkeit wurde auch unter Anwendung des Home-Office-Konzepts ständig unter Beweis gestellt. Die Vorbereitungen für das 50-jährige Jubiläum des Hessischen Datenschutzgesetzes, die schon sehr weit gediehen waren, mussten leider abgebrochen werden. So wie es aussieht, müssen wir die Vorbereitungen auf das 60-jährige Jubiläum erstrecken. Die sachgerechte Behandlung von Eingaben auch unter Berücksichtigung der Kontaktsperreanforderungen

dürfte dazu beigetragen haben, dass die Betroffenen die Einschränkungen ihrer informationellen Selbstbestimmung verständnisvoll hinnahmen.

2. Europa, Internationales

2.1
Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden nach Kapitel VII DS-GVO sowie Mitarbeit in Arbeitsgremien der DSK und des EDSA (s. a. 47. und 48. Tätigkeitsbericht, Ziff. 4.2.2 und Ziff. 3.2)

Mit Inkrafttreten der DS-GVO haben sich, wie bereits im 47. und 48. Tätigkeitsbericht geschildert, zahlreiche Neuerungen für die Zusammenarbeit der Aufsichtsbehörden in Deutschland und Europa ergeben. Die DS-GVO verpflichtet die europäischen Datenschutzaufsichtsbehörden, in Fällen grenzüberschreitender Datenverarbeitungen eng zu kooperieren. Um den kommunikativen und organisatorischen Mehraufwand zu bewältigen, der sich aus der Intensivierung der Zusammenarbeit ergibt, hat der HBDI im Jahr 2019 die Stabsstelle Europa und Internationales neu eingerichtet, die als Bindeglied zwischen dem HBDI und verschiedenen Stellen außerhalb Hessens in Deutschland, Europa und der Welt fungiert.

Alle beim HBDI eingehenden Beschwerden, Anfragen und Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO werden in den Fachreferaten zunächst daraufhin überprüft, ob eine grenzüberschreitende Verarbeitung vorliegt, welche die Pflicht zur Zusammenarbeit mit anderen europäischen Aufsichtsbehörden auslöst. Eine grenzüberschreitende Verarbeitung liegt gemäß Art. 4 Nr. 23 DS-GVO vor, wenn der Verantwortliche bzw. Auftragsverarbeiter in mehreren Mitgliedstaaten niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt oder wenn es nur eine einzelne Niederlassung in der EU gibt, aber die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Verfahren der Kooperation und Kohärenz nach Kapitel VII DS-GVO

Nicht erst seit Inkrafttreten der DS-GVO gehen beim HBDI neben Beschwerden gegen hessische Unternehmen und Behörden vermehrt auch Beschwerden gegen Unternehmen mit Sitz in anderen EU-Mitgliedstaaten ein. Nach dem mit der DS-GVO neu eingeführten Konzept des sog. One-Stop-Shop ist bei grenzüberschreitenden Datenverarbeitungen eine Aufsichtsbehörde (i. d. R. die Aufsichtsbehörde der Hauptniederlassung des Verantwortlichen bzw. Auftragsverarbeiters, Art. 56 Abs. 1 DS-GVO) als 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 alleine entscheidet. Vielmehr wirken neben der federführenden Aufsichtsbehörde auch alle weiteren betroffenen Aufsichtsbehörden an der Entscheidungsfindung mit. „Betroffen" („concerned") sind nach Art. 4 Nr. 22 DS-GVO alle Aufsichtsbehörden der Mitgliedstaaten, in deren Hoheitsgebiet der Verantwortliche bzw. Auftragsverarbeiter niedergelassen ist, individuell betroffene Personen („data subjects") ihren Wohnsitz haben oder bei denen eine Beschwerde eingereicht wurde. Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden arbeiten im Kooperationsverfahren eng zusammen und versuchen, einen Konsens zu erzielen (Art. 60 Abs. 1 DS-GVO). Die federführende Aufsichtsbehörde prüft den Fall und legt den betroffenen Aufsichtsbehörden einen Beschlussentwurf vor (Art. 60 Abs. 3 Satz 2 DS-GVO). Gegen diesen Beschlussentwurf können die betroffenen Aufsichtsbehörden Einspruch einlegen (Art. 60 Abs. 4 DS-GVO). Bei unlösbaren Meinungsverschiedenheiten wird die Angelegenheit dem Europäischen Datenschutzausschuss (EDSA) im Kohärenzverfahren nach Art. 63 DS-GVO zur verbindlichen Entscheidung vorgelegt.

Die Zusammenarbeit, Abstimmung und Kommunikation in grenzüberschreitenden Verwaltungsverfahren erfolgt elektronisch über das sog. IMI-System (Internal Market Information System, deutsch: Binnenmarkt-Informationssystem). Bei den europäischen Datenschutzaufsichtsbehörden eingehende Beschwerden und Meldungen nach Art. 33 DS-GVO mit grenzüberschreitendem Bezug werden in einem ersten Schritt in einem Verfahren nach Art. 56 DS-GVO zur Feststellung der federführenden und betroffenen Aufsichtsbehörden in das IMI-System eingestellt. Dabei ist der Sachverhalt für die anderen Aufsichtsbehörden in englischer Sprache (EDSA-Papier „GDPR in IMI – User Guide For Supervisory Authorities": „All cooperation procedures should be documented in English.") zusammengefasst zu schildern und die mutmaßlich federführende sowie die mutmaßlich betroffenen Aufsichtsbehörden anzugeben. Die übrigen Aufsichtsbehörden haben dann Gelegenheit, den Fall zu prüfen und sich innerhalb eines Monats als federführende oder betroffene Aufsichtsbehörde zu melden.

Wird im Art. 56-Verfahren festgestellt, dass die europäische Federführung beim HBDI liegt, leitet die Stabsstelle Europa und Internationales die über das IMI-System eingegangene Beschwerde nebst weiterer Unterlagen an das jeweilige Fachreferat weiter, welches dann nach eingehender Prüfung des Sachverhalts die Beschwerde bearbeitet und Kontakt zum Verantwortlichen aufnimmt.

Für den Fall, dass die Federführung bei einer anderen europäischen Aufsichtsbehörde liegt, übermittelt die Stabsstelle Europa und Internationales die Beschwerde zur Bearbeitung an die betreffende Behörde. Hierzu müssen die Beschwerde sowie alle weiteren zur Bearbeitung notwendigen Unterlagen und sachdienlichen Informationen ins Englische übersetzt werden, da die Kommunikation zwischen den verschiedenen Aufsichtsbehörden im IMI-System auf Englisch erfolgt.

Gestiegene Fallzahlen und erhöhter Prüfungsaufwand

Die Zahl der über das IMI-System gemeldeten Beschwerden, Art. 33-Meldungen und Amtsermittlungsverfahren stieg im Berichtszeitraum im Vergleich zum Vorjahr weiter an, s. a. Teil I Ziff. 15.1, 17.1 und 17.2. Im Berichtszeitraum waren von der Stabsstelle Europa und Internationales insgesamt 759 im IMI-System eingetragene Art. 56-Verfahren auf eine mögliche Betroffenheit bzw. Federführung zu prüfen. In 198 dieser Verfahren hat die Stabsstelle Europa und Internationales den HBDI als „betroffen“ gemeldet, befasst sich in der Folge inhaltlich mit der Angelegenheit und wirkt an der Entscheidungsfindung mit. In weiteren fünf Verfahren hat der HBDI die Bearbeitung der Beschwerde als federführende Aufsichtsbehörde übernommen. Zudem hat die Stabsstelle Europa und Internationales 42 beim HBDI eingegangene Beschwerden zur weiteren Bearbeitung als Federführung an andere europäische Aufsichtsbehörden übermittelt. In diesen Verfahren wirkt der HBDI als betroffene Aufsichtsbehörde an der Entscheidungsfindung mit und bleibt im sog. One-Stop-Shop-Verfahren Ansprechpartner für die Beschwerdeführerin oder den Beschwerdeführer und informiert in regelmäßigen Abständen über den Stand der Bearbeitung.

In 290 grenzüberschreitenden Verwaltungsverfahren wurden im Berichtszeitraum von den europäischen Aufsichtsbehörden Beschlussentwürfe nach Art. 60 Abs. 3 Satz 2 DS-GVO in das IMI-System eingestellt, die von der Stabsstelle Europa und Internationales gemeinsam mit den jeweiligen Fachreferaten im Hinblick auf mögliche Bedenken und die Einlegung eines Einspruchs zu prüfen waren. Zudem hat die Stabsstelle Europa und Internationales den anderen europäischen Aufsichtsbehörden 22 eigene Beschlussentwürfe vorgelegt.

201 Verfahren, in denen der HBDI als betroffene Aufsichtsbehörde beteiligt war, konnten im Berichtsjahr mit einer abschließenden Entscheidung abgeschlossen werden, davon acht Fälle mit hessischer Federführung.

Auch die Zahl der Verfahren der gegenseitigen Amtshilfe nach Art. 61 DS-GVO nimmt weiter zu. Im Berichtszeitraum hat die Stabsstelle Europa und Internationales 271 Amtshilfeersuchen anderer europäischer Aufsichtsbe-

hörden bearbeitet und 15 eigene Amtshilfeersuchen an andere Aufsichtsbehörden gestellt.

Im neuen Jahr dürfte die Zahl der vom HBDI zu bearbeitenden Kooperationsverfahren weiter steigen. Nicht zuletzt auch aufgrund des Austritts Großbritanniens aus der EU, der in einigen grenzüberschreitenden Verwaltungsverfahren dazu führt, dass die Federführung von der britischen Datenschutzaufsichtsbehörde auf den HBDI wechselt.

Binding Corporate Rules-Genehmigungsverfahren

Neben den über das IMI-System zu bearbeitenden grenzüberschreitenden Verwaltungsverfahren liegt ein weiterer Schwerpunkt der Tätigkeit der Stabsstelle Europa und Internationales in der Prüfung und Genehmigung von Binding Corporate Rules (deutsch: verbindliche interne Datenschutzvorschriften; kurz: BCR), die sich – auch aufgrund des sog. Schrems II-Urteils des EuGH (EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18) und der Unwirksamkeit des EU-US Privacy Shields – als Transferinstrument wachsender Beliebtheit erfreuen.

BCR sind komplexe Vertragswerke mit Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein multinationaler Konzern 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.

Die BCR-Unterlagen werden in einem europaweiten Kooperationsverfahren 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, bevor der EDSA eine Stellungnahme hierzu abgibt.

Erst wenn diese Stellungnahme positiv ausfällt, kann eine Genehmigung durch den BCR Lead erfolgen, die dann für die übrigen Aufsichtsbehörden bindend ist. Alle europäischen Aufsichtsbehörden werden damit stärker in die Verantwortung und 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 100 Anträge auf Genehmigung von BCR anhängig. Für 13 dieser BCR-Verfahren ist der HBDI europaweit als sog. BCR Lead federfüh-

rend zuständig. Davon wurden fünf BCR-Genehmigungsverfahren infolge des Brexits von der britischen Datenschutzaufsichtsbehörde als neuer BCR Lead übernommen. In 27 weiteren BCR-Verfahren hat der HBDI die Federführung innerhalb Deutschlands und in zwei Verfahren die Co-Prüfung übernommen.

Mitarbeit in Gremien der DSK und auf Ebene des EDSA sowie Informationsweitergabe beim HBDI

Über ihre Aufgaben in grenzüberschreitenden Verwaltungsverfahren und bei der Prüfung von BCR hinaus unterstützt die Stabsstelle Europa und Internationales auf nationaler und europäischer Ebene verschiedene Arbeitsgremien der DSK bzw. Arbeitsgruppen des EDSA. Hierzu gehört die Übernahme der Vertretung Deutschlands auf Ebene des EDSA in der International Transfers Subgroup. Die International Transfers Subgroup befasst sich mit internationalen Datentransfers und sämtlichen Themen und Fragen, die sich auf diesem Gebiet stellen. Neben der Teilnahme an regelmäßigen Sitzungen der Subgroup und BCR-Sessions engagiert sich die Stabsstelle Europa und Internationales auf europäischer Ebene in diversen Drafting Teams und Task Forces und berichtet gemeinsam mit Kolleginnen und Kollegen des LDA Bayern und des BfDI den deutschen Aufsichtsbehörden stetig über die Arbeit der Subgroup und die Entwicklungen auf dem Gebiet des europäischen und internationalen Datenschutzrechtes. Die Rückmeldungen aus den deutschen Aufsichtsbehörden bringt der HBDI als Ländervertreter dann wiederum in die Diskussionen auf europäischer Ebene ein. So gelingt es z. B., Einfluss auf vom EDSA zu verabschiedende Leitlinien und Empfehlungen zu nehmen, die dann für die spätere aufsichtsbehördliche Tätigkeit aller Beteiligten maßgeblich und richtungsweisend werden.

Neben den Informationen aus der International Transfers Subgroup sichtet die Stabsstelle Europa und Internationales aber auch sämtliche Posteingänge aus den übrigen Subgroups des EDSA (z. B. Arbeitspapiere und -ergebnisse, Tagesordnungen und Protokolle), welche die Stabsstelle zum Teil per E-Mail, aber auch elektronisch über Confluence, das Kollaborations-Tool des EDSA, erreichen. Monatlich gehen aus Europa allein aus diesen Subgroups über 100 E-Mails im Postfach der Stabsstelle Europa und Internationales ein, die nach Durchsicht und inhaltlicher Prüfung an die jeweils zuständigen Fachreferate beim HBDI – sei es zur bloßen Information und Kenntnis oder gegebenenfalls weiteren Veranlassung – weitergeleitet werden müssen. Dies versetzt die Fachreferate des HBDI in die Lage, sich aktiv und gestaltend in die Arbeiten auf europäischer Ebene einzubringen und z. B. durch Mitarbeit in ad-hoc-Gruppen oder frühzeitige Kommentierung von Papieren, die sich

im Entwurfsstadium befinden, Einfluss auf den Meinungsbildungsprozess im EDSA zu nehmen.

Auch auf nationaler Ebene ist der HBDI durch die Stabsstelle Europa und Internationales in Arbeitsgremien der DSK vertreten. So liegt die Leitung des bundesweiten Arbeitskreises Organisation und Struktur bei der Stabsstelle Europa und Internationales. Der Arbeitskreis Organisation und Struktur unterstützt die Arbeit der DSK in wichtigen organisatorischen Fragestellungen und entwickelt Konzepte und Prozesse zur besseren Verzahnung der Arbeit auf deutscher und europäischer Ebene. Ein weiterer Themenkreis, mit dem sich der Arbeitskreis intensiv beschäftigt, sind Fragen, die sich aus der europäischen Zusammenarbeit nach Kapitel VII der DS-GVO ergeben, einschließlich der konkreten Abwicklung dieser Verfahren im IMI-System. Neben der Organisation regelmäßiger Arbeitskreissitzungen hat die Stabsstelle Europa und Internationales hier stetig die Entwicklungen auf nationaler und europäischer Ebene zu beobachten und zu bewerten, um den Kolleginnen und Kollegen der deutschen Aufsichtsbehörden berichten zu können. Daneben nimmt die Stabsstelle Europa und Internationales für den HBDI auch an den Sitzungen des Arbeitskreises Internationaler Datenverkehr teil. Als Vertreter in der International Transfers Subgroup kommt dem HBDI auch in diesem Arbeitskreis eine nicht zu unterschätzende Funktion zu.

Fazit und Ausblick

Neben den Kooperations- und Kohärenzverfahren nach Kapitel VII DS-GVO bündelt eine Vielzahl von kommunikativen und organisatorischen Aufgaben die Arbeitskraft der Stabsstelle Europa und Internationales. Die Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden hat sich im zweiten Jahr nach Inkrafttreten der DS-GVO weitgehend eingespielt. Die stetig steigende Zahl der grenzüberschreitenden Verwaltungsverfahren und BCR-Anträge stellt für den HBDI und die anderen deutschen und europäischen Datenschutzaufsichtsbehörden aber nach wie vor eine Herausforderung und einen erheblichen kommunikativen und organisatorischen Mehraufwand dar. Nicht zuletzt aufgrund der Mitarbeit in Arbeitsgremien, Drafting Teams und Task Forces auf nationaler und europäischer Ebene, dem Austritt Großbritanniens aus der EU und den noch nicht in allen Einzelheiten abzusehenden Auswirkungen des sog. Schrems II-Urteils des EuGH auf Drittlanddatentransfers ist in den kommenden Jahren mit einem weiteren deutlichen Anstieg des Beratungs- und Prüfungsaufwandes für die Stabsstelle Europa und Internationales zu rechnen.

2.2
Internationale Datentransfers – Privacy Shield ungültig, neue Standarddatenschutzklauseln in Arbeit

Mit einer richtungsweisenden Entscheidung (C-311/18, Schrems II) hat der EuGH für erhebliche Verunsicherung bei Datentransfers in Drittstaaten gesorgt. Um den Datenexporteuren hierzu Orientierung und Unterstützung zu bieten, arbeitet der HBDI als Mitglied der Taskforce des Europäischen Datenschutzausschusses (EDSA) intensiv an der Erarbeitung europaweit abgestimmter Empfehlungen zu Maßnahmen mit, welche die Instrumente für Übermittlungen personenbezogener Daten in Drittländer ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten.
Gleichzeitig hat die Europäische Kommission Entwürfe für sogenannte Standarddatenschutzklauseln entworfen und dem EDSA zur Stellungnahme vorgelegt. An deren Erarbeitung ist der HBDI als ständiger Vertreter der Expertenarbeitsgruppe zu internationalen Datentransfers des EDSA und Mitglied im Autorenteam beteiligt.

Auch in diesem Berichtsjahr hätte wieder eine Überprüfung des EU-U.S. Privacy Shields angestanden (Bericht über die vorangegangenen Prüfungen: 48. TB, Ziff.3.1, S. 7f; 47. TB, Ziff. 4.2.1, S. 94ff. und 46. TB, Ziff. 4.1, S. 55 ff.). Diese wurde jedoch obsolet, weil der EuGH mit seiner Entscheidung vom 16.07.2020 den dem Privacy Shield zugrundeliegenden Beschluss der Europäischen Kommission für ungültig erklärt hat. Die Folgen dieses Urteils sind sehr weitreichend und stellen nicht nur Datentransfers von der EU in die USA in Frage: Im Ergebnis bürdet der EuGH Datenexporteuren in der EU, die personenbezogene Daten nach außerhalb der EU verbringen möchten, enorme zusätzliche Prüfpflichten auf. Wo man sich bislang auf eine Privacy Shield-Zertifizierung des Empfängers in den USA verlassen oder sogenannte Standardvertragsklauseln (die unter der DS-GVO nun Standarddatenschutzklauseln heißen) abgeschlossen hat, um für einen Schutz der Daten auch im Empfängerland zu sorgen, verlangt der EuGH jetzt erheblich mehr.

Im Wesentlichen muss jeder Datenexporteur im konkreten Fall prüfen, ob der oder die Datenempfänger im Drittland auch in der Lage sind, die in den Standarddatenschutzklauseln getroffenen Vereinbarungen (oder die Vereinbarungen eines anderen Instruments für Übermittlungen personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO) auch tatsächlich einzuhalten. Das bedeutet, dass überprüft werden muss, ob im Drittstaat etwa Gesetze existieren, die den Datenempfänger daran hindern könnten, einzelne Vereinbarungen zu befolgen. Hier kommen grundsätzlich alle gesetzlichen Regelungen und Praktiken im Drittland in Frage, die das durch

das *Instrument für Übermittlungen personenbezogener Daten in Drittländer* geschaffene Schutzniveau negativ beeinflussen könnten. Besonderen Fokus legt der EuGH auf Vorschriften, die öffentlichen Stellen des Drittlandes Zugriff auf die übermittelten Daten gewähren. Gehen solche über das Maß, das in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, hinaus oder bestehen für die Betroffenen keine durchsetzbaren Rechte und kein wirksamer Rechtsschutz gegen solche Maßnahmen, muss sich der Datenexporteur überlegen, ob und wie er diese Defizite des Datenschutzniveaus im Empfängerland ausgleichen kann. Hierzu führt der EuGH sogenannte „zusätzliche Maßnahmen" ins Feld, ohne jedoch näher auszuführen, worin diese bestehen können. Er führt jedoch weiter aus, dass ein Transfer, bei dem die Daten einem solchen identifizierten Risiko ausgesetzt sind, das sich durch zusätzliche Maßnahmen nicht auf ein Schutzniveau bringen lässt, das demjenigen innerhalb der EU dem Wesen nach gleichwertig ist, nicht stattfinden darf und daher vom Datenexporteur vermieden, ausgesetzt oder beendet werden muss.

Die Last, diese Prüfungen vorzunehmen, erlegt der EuGH zuvörderst den Datenexporteuren auf. Um diese hierbei zu unterstützen, arbeitet der EDSA derzeit an umfangreichen Empfehlungen zum Umgang mit internationalen Datentransfers unter Berücksichtigung der vom EuGH in seinem Urteil aufgestellten Anforderungen nebst zusätzlichen Maßnahmen, welche die Transfer-Tools aus Kapitel V DS-GVO ergänzen, um die Einhaltung des Schutzniveaus für personenbezogene Daten zu gewährleisten. Diese sind unter *https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/EDPB%20Recommendations%2001_2020%20Supplementary%20Measures%20EN.pdf* zu finden. Ein weiteres Papier, das sich näher mit den Anforderungen an staatliche Zugriffe zu Überwachungszwecken befasst, ist hier zu finden: *https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/EDPB%20Recommendations%2002_2020%20Essential%20Guarantees%20Surveillance%20Measures%20EN.pdf.*

Beide Papiere befinden sich derzeit jedoch noch in einer öffentlichen Anhörung. Dem Aufruf zur Abgabe von Stellungnahmen wurde in erheblichem Umfang gefolgt. Zum erstgenannten Papier sind insgesamt 207 Stellungnahmen eingegangen. Sie umfassen etwa 1500 Seiten und sind nun zu sichten und zu diskutieren, um zu entscheiden, ob und inwieweit das Papier daraufhin überarbeitet werden sollte. Hierbei sind stets alle beteiligten Datenschutzaufsichtsbehörden einzubinden, das heißt alle 27 europäischen und auch sämtliche deutschen Aufsichtsbehörden. Deren ständige Information und Einbeziehung in europäische Diskussions- und Abstimmungsprozesse gehören auf dem Gebiet der internationalen Datentransfers genauso zu den Aufgaben wie die eigentliche fachliche Arbeit in den europäischen Gremien.

Auch auf das Urteil hin hat die Europäische Kommission (KOM) daneben die Standarddatenschutzklauseln überarbeitet und dem EDSA im Rahmen des Verfahrens zum Erlass eines neuen Beschlusses der KOM zur Stellungnahme vorgelegt: *https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.*

An der Erarbeitung der Stellungnahme des EDSA zu diesen Standarddatenschutzklauseln ist der HBDI als Mitglied des Autorenteams der Expertengruppe auf europäischer Ebene ebenfalls intensiv beteiligt. Die vom EDSA verabschiedete Stellungnahme hierzu findet sich unter *https://edpb.europa.eu/our-work-tools/consistency-findings/edpbedps-joint-opinions_en.*

Das Urteil und seine Auswirkungen werden den HBDI noch eine ganze Weile intensiv beschäftigen. So sind sämtliche existierenden Leitlinien und sonstige Papiere, die auf deutscher und europäischer Ebene zu dieser Thematik existieren, zu überarbeiten. Das Urteil hat einige Aufmerksamkeit erregt, so dass zu diesem Thema eingegangene Beratungsanfragen und Beschwerden zu bearbeiten sein werden. Schließlich hat die KOM bereits angekündigt, dass auch alle bereits bestehenden Adäquanzentscheidungen (derzeit existieren zwölf, die hier zu finden sind: *https://datenschutz.hessen.de/datenschutz/internationales/angemessenheitsbeschl%C3%BCsse*) an den durch den EuGH in seinem Urteil gesetzten Maßstäben überprüft werden. Auch zu diesen Überprüfungen werden Stellungnahmen des EDSA erarbeitet werden müssen. Schließlich steht die Übermittlung eines Entwurfes für eine Adäquanzentscheidung für das Vereinigte Königreich (UK) unmittelbar bevor. Auch zu dieser wird eine umfangreiche Stellungnahme durch die Experten des EDSA zu erstellen sein.

3. Allgemeine Verwaltung, Kommunen

3.1
Datenspeicherung von Schwimmbadbesuchern

Die Speicherung von Name und Anschrift der Besucher von kommunalen Schwimmbädern ist rechtlich nicht zulässig, da der Verordnungsgeber dafür wegen fehlenden Erfordernisses bewusst keine Rechtsgrundlage geschaffen hat.

Als zu Beginn des Sommers in Hessen die Freibäder wieder öffneten, wurde ich von verschiedenen hessischen Kommunen danach gefragt, ob sie von den Besuchern der Schwimmbäder beim Zutritt Name und Anschrift erheben und ob sie diese Daten einen Monat aufbewahren müssten, wie dies bei den Restaurantbetreibern erforderlich sei.

Außerdem erreichten mich einige Bürgeranfragen, mit denen Beschwerde geführt wurde, dass bei der Online-Terminvergabe für einen Schwimmbadbesuch nicht nur Name und Anschrift, sondern auch Geburtsdatum und Telefonnummer abgefragt wurden.

Die Fragestellungen schienen sich zu gleichen, waren aber rechtlich zu unterscheiden.

Den anfragenden Kommunen musste ich mitteilen, dass es für die Erhebung von Name und Anschrift der Schwimmbadbesucher und der Aufbewahrung dieser Daten für die Dauer eines Monats zum Zwecke der Kontaktverfolgung keine Rechtsgrundlage gibt; denn anders als für Restaurantbetreiber und Veranstalter von Festen enthielt die Corona-Kontakt- und Betriebsbeschränkungsverordnung für die Besuche von Schwimmbädern keine Regelung. Anlässlich der Anfragen durch die Kommunen hatte ich sowohl mit dem Hessischen Ministerium für Wirtschaft, Energie, Verkehr und Wohnen als auch mit dem Hessischen Ministerium für Soziales und Integration Kontakt aufgenommen, um die Problematik zu erörtern. Aus dem Sozialministerium wurde mir daraufhin mitgeteilt, dass der Verordnungsgeber hier bewusst auf die Regelung zur Erhebung personenbezogener Daten verzichtet habe, weil man bei Schwimmbadbesuchen bei Einhaltung von Hygienevorgaben keine erhöhte Ansteckungsgefahr befürchtete, so dass ein Erfordernis der Kontaktverfolgung nicht bestehe.

Bei der Online-Terminvergabe, mit der im Vorhinein die Anzahl der Besucher von Schwimmbädern gesteuert werden sollte, habe ich hingegen die Angabe von Namen und Anschrift für die Zutrittskontrolle für zulässig gehalten. Allerdings ist auch hier die Speicherung der Daten nach dem Schwimmbad-

besuch als unzulässig anzusehen. Die Erhebung des Geburtsdatums ist für die Zugangssteuerung nicht erforderlich und hat deshalb zu unterbleiben. Dies habe ich den Schwimmbadbetreibern mitgeteilt.

3.2
Recht auf Vergessenwerden – Löschung der Namen von Mandatsträgern aus Sitzungsprotokollen unter Berufung auf die DS-GVO

Ehemalige Gemeindevertreter haben keinen Anspruch auf Löschung ihrer Namen aus Sitzungsprotokollen. Hingegen müssen sie eine Veröffentlichung der Sitzungsprotokolle mit namentlicher Nennung im Internet nicht hinnehmen.

Im Hessischen Landtag wurde eine Kleine Anfrage gestellt, ob ehemalige Gemeindevertreter gemäß Art. 17 DS-GVO einen Anspruch darauf haben, dass ihre Namen aus Sitzungsprotokollen der Gemeindevertretungen gelöscht werden. Das Hessische Ministerium des Innern und für Sport hat seine Antwort mit mir abgestimmt.

Vorausgegangen war die Berichterstattung einer Frankfurter Zeitung, dass in Friedberg ein ehemaliger Stadtverordneter unter Bezug auf die DS-GVO verlangt hatte, dass sein Name aus sämtlichen Sitzungsprotokollen der Stadtverordnetensitzungen entfernt werde. Die Stadt ist diesem Verlangen gefolgt und hat den Namen sowohl aus allen elektronischen Dokumenten gelöscht, als auch in allen Sitzungsunterlagen in Papierform geschwärzt, was einen nicht unerheblichen Aufwand bedeutete. Die Kleine Anfrage an die Landesregierung zielte darauf zu erfahren, ob dieses Ansinnen schon öfters gestellt wurde und ob die Landesregierung hier Regelungsbedarf sieht.

Unabhängig von der Einbeziehung bei der Beantwortung dieser Kleinen Anfrage hatte sich auch an den HBDI ein ehemaliger Stadtverordneter aus einer anderen Kommune gewandt, der ebenfalls die Löschung seiner Daten aus alten Protokollen unter Berufung auf die DS-GVO verlangte.

Bei der Bewertung der Frage, ob ein Anspruch auf Löschung der personenbezogenen Angaben in den Sitzungsprotokollen besteht, ist zwischen den Sitzungsprotokollen, die sich in den Archiven der Gemeindevertretungen befinden, und der Veröffentlichung von Sitzungsprotokollen im Internet zu unterscheiden.

Wie schon das HMDIS in seiner Antwort auf die Kleine Anfrage (LT-Drs. 20/3107) ausführte, ergibt sich die Pflicht zur Protokollierung der Sitzungen der Gemeindevertretung aus der Hessischen Gemeindeordnung (HGO). Nach § 61 Abs. 1 Satz 2 HGO muss die Niederschrift ausdrücklich auch die Namen

der in der Sitzung Anwesenden enthalten. Solange die Protokolle aufbewahrt werden müssen, sind auch die Namen der anwesenden Sitzungsteilnehmer als Bestandteil der Protokolle aufzubewahren. Nach Ablauf der Aufbewahrungsfristen werden die Protokolle nach den archivrechtlichen Vorschriften aufbewahrt. Wenn hier eine dauerhafte Archivierung vorgesehen ist, werden auch die Namen der Sitzungsteilnehmer dauerhaft archiviert. Ein Löschanspruch aus Art. 17 Abs. 3 lit. d DS-GVO besteht nicht. Die Archivierung liegt im öffentlichen Interesse.

Hingegen gibt es für eine Veröffentlichung der Sitzungsprotokolle im Internet unter Nennung der anwesenden Sitzungsteilnehmer keine Rechtsgrundlage, da die HGO eine derartige Veröffentlichung nicht vorsieht. Deshalb ist eine solche Veröffentlichung nur mit einer ausdrücklich erklärten Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO rechtlich zulässig. Sollte eine Internetveröffentlichung ohne eine solche Einwilligung erfolgt sein, dann steht den davon Betroffenen auch ein Recht auf Löschung gemäß Art. 17 Abs. 1 lit. d DS-GVO zu.

3.3
Besonderes Behördenpostfach

Die Einrichtung nur eines besonderen Behördenpostfaches pro Kommune ist datenschutzrechtlich nicht akzeptabel.

Nach § 6 Abs. 1 der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere Behördenpostfach (ERVV) können die Behörden sowie juristische Personen des öffentlichen Rechts (Postfachinhaber) zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg ein besonderes elektronisches Behördenpostfach verwenden, das zur Kommunikation mit den Gerichten dient.

Durch die Stadt Frankfurt wurde ich darauf aufmerksam gemacht, dass die Hessische Zentrale für Datenverarbeitung (HZD) pro Kommune jeweils nur ein solches Behördenpostfach einrichten will. Die Stadt hat dies aus datenschutzrechtlicher Sicht problematisiert und die Einrichtung eines zentralen Postfaches beim Hauptamt für alle anderen Ämter (Sozialamt, Jugendamt, Gesundheitsamt etc.) als datenschutzrechtlichen Rückschritt bezeichnet, da bisher die Ämter einzeln adressierbar seien. Gerade dort, wo besonders sensible Daten verarbeitet würden, würde durch die „zentrale Poststelle“ beim besonderen Behördenpostfach eine Stelle Kenntnis von Daten erlangen, die ihr bisher nicht zugänglich gewesen seien.

Ich habe mich dieser Auffassung angeschlossen und meine Bedenken gegenüber der HZD vorgetragen. Diese argumentierte, dass die Beschränkung auf nur ein besonderes elektronisches Behördenpostfach pro Behörde sich unmittelbar aus § 6 ERVV ergebe, da dort von den Behörden und „einem" Postfach gesprochen werde. Jede Behörde gebe es nur einmal und der Begriff der Behörde sei im Kontext der Prozessordnungen auszulegen, d. h., der Begriff sei der Gesamtbehörde zuzurechnen. Zudem wurde angeführt, dass mit der Einrichtung mehrerer besonderer Behördenpostfächer bei einer Kommune das Risiko von Fehladressierungen steige.

Die von der HZD vorgenommene Auslegung des Behördenbegriffs ist datenschutzrechtlich nicht haltbar. Ich habe in meinen Tätigkeitsberichten schon in der Vergangenheit ausgeführt, dass aus Sicht des Datenschutzes vom funktionalen Behördenbegriff auszugehen ist. Dies habe ich gegenüber dem Hessischen Ministerium für Digitale Strategie und Entwicklung vorgetragen und insbesondere Folgendes hervorgehoben:

– Auch bei der von der HZD vorgenommenen Auslegung des Behördenbegriffs wird die Ausländerbehörde nicht zum Gesundheitsamt oder umgekehrt. Beide sind datenschutzrechtlich eigene verantwortliche Stellen (wenn auch unter dem Dach der Stadtverwaltung), die mit völlig unterschiedlichen Rechtsgrundlagen arbeiten und die entsprechend der Vorgaben aus Art. 5 Abs. 1, 24, 25 und 32 DS-GVO sicherzustellen haben, dass ihre Daten nicht ohne entsprechende Rechtsgrundlagen an das jeweilige Amt übermittelt werden. Gerade dies wäre jedoch bei einem zentralen Behördenpostfach der Fall. Alle Daten liefen über das Hauptamt. Eine Stadtverwaltung ist jedoch gerade keine informationelle Einheit.

Im Übrigen habe ich das Ministerium darauf aufmerksam gemacht, dass der Hinweis des Bundesjustizministeriums, dass es pro Behörde nur ein besonderes Behördenpostfach geben könne, keineswegs deutschlandweit befolgt werde, da sowohl für Bundesbehörden als auch für Kommunen in anderen Bundesländern längst mehrere besondere Behördenpostfächer nach § 6 ERVV eingerichtet worden seien.

Eine Regelungskompetenz für die Kommunen steht dem Bund ohnehin nicht zu.

Die Staatsministerin für Digitale Strategie und Entwicklung hatte mir zwischenzeitlich mitgeteilt, dass sich in den Bundesländern durch eine zunehmende Diskussion eine Veränderung der bisherigen, vom Bundesjustizministerium formulierten Position abzeichne. So könne beispielsweise in begründeten Ausnahmefällen und nach Festlegung einheitlicher Kriterien eine Abweichung von der „Ein-Postfach-Strategie" überlegenswert sein.

Inzwischen teilte mir das Ministerium mit, dass grundsätzlich die Einrichtung eines besonderen Behördenpostfachs pro Amt als unkritisch angesehen werde und dem sog. „funktionalen Behördenbegriff“ entspreche. Die Erstellung der Kriterien für die Vergabe mehrerer besonderer elektronischer Behördenpostfächer für eine Kommune sowie die praktische Umsetzung dieser Vergabe werde derzeit erarbeitet.

3.4
Beauftragung externer Dienstleister im Rahmen des § 6a Abs. 3 KAG

Die Beauftragung externer Dienstleister im Rahmen von § 6a KAG unterliegt den allgemeinen datenschutzrechtlichen Bestimmungen.

Im Sommer 2020 meldeten sich mehrere Bürger und beschwerten sich über ein Anschreiben ihrer Kommunalverwaltung zur Einführung eines wiederkehrenden Straßenbeitrages. In diesem Anschreiben wurden die Bürgerinnen und Bürger aufgefordert, Angaben zu ihren Grundstücken und deren konkrete Bebauung zu machen. Hierzu sollte ein beigefügter Fragebogen ausgefüllt werden und an einen von der Kommune beauftragten privaten Dienstleister übersandt werden. Die Beschwerdeführer trugen Vorbehalte gegen diese Vorgehensweise vor und fragten, ob diese Verfahrensweise rechtlich zulässig sei und ob sie verpflichtet seien, gegenüber einem beauftragten Dienstleister ihre personenbezogenen Daten zu offenbaren. In dem mir exemplarisch zugesandten siebenseitigen Anschreiben fand sich keine Erläuterung zur Vorgehensweise unter Beauftragung des externen Dienstleisters und auch kein diesbezüglicher datenschutzrechtlicher Hinweis.

Eine grundsätzliche Möglichkeit zur Beauftragung externer Dienstleister besteht im Rahmen der Vorschrift des § 6a Abs. 3 des Gesetzes über kommunale Abgaben (KAG).

§ 6a KAG

(1) Die Festsetzung und Erhebung mehrerer Abgaben, die denselben Abgabenpflichtigen betreffen, können in einem Bescheid zusammengefasst werden.

(2) Ein Bescheid über Abgaben für einen bestimmten Zeitabschnitt kann bestimmen, dass er auch für künftige Zeitabschnitte gilt, solange sich die Berechnungsgrundlagen und der Abgabenbetrag nicht ändern. Abgabenbescheide mit Dauerwirkung sind von Amts wegen aufzuheben oder zu ändern, wenn die Abgabenpflicht entfällt oder sich die Höhe der Abgaben ändert.

(3) Die Gemeinden und Landkreise können in ihren Gebühren- und Beitragssatzungen bestimmen, dass die Ermittlung von Berechnungsgrundlagen, die Abgabenberechnung, die Ausfertigung und Versendung von Abgabenbescheiden sowie die Entgegennahme der

zu entrichtenden Abgaben von einem damit beauftragten Dritten wahrgenommen werden. Der Dritte darf nur beauftragt werden, wenn die ordnungsgemäße Erledigung und Prüfung nach den für die Gemeinden und Landkreise geltenden Vorschriften gewährleistet ist. Die Gemeinden und Landkreise können sich zur Erledigung der in Satz 1 genannten Aufgaben auch der Datenverarbeitungsanlagen Dritter bedienen.

Aus der Vorschrift ergeben sich zunächst unmittelbar die Voraussetzungen, welche die beteiligten Stellen zu erfüllen haben. Seitens des beauftragten Dienstleisters muss die Einhaltung der geltenden Vorschriften der Gemeinden und Landkreise gewährleistet sein und die beauftragende Kommune muss ihre Gebühren- und Beitragssatzungen entsprechend formuliert haben.

Neben den Voraussetzungen, die sich unmittelbar aus der Vorschrift des § 6a KAG ergeben, bedürfen die korrespondierenden Datenübermittlungen zwischen Kommune und beauftragtem Dienstleister der Beachtung datenschutzrechtlicher Regelungen, soweit dort personenbezogene Daten verarbeitet werden. Dies muss nicht zwangsläufig der Fall sein, im betreffenden Sachverhalt sollten jedoch personenbezogene Daten an den beauftragten Dienstleister übermittelt werden. Daher ist hier eine Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO gesetzlich geboten. Soweit den rechtlichen Vorschriften entsprochen wird, ist ein solches Vorgehen im Zusammenhang mit der Einführung eines wiederkehrenden Straßenbeitrages grundsätzlich rechtlich zulässig.

Die weitere Fragestellung war, ob die Bürgerinnen und Bürger in einem solchen Zusammenhang von der Kommunalverwaltung verpflichtet werden können, die personenbezogenen Daten unmittelbar an den beauftragten Dienstleister zu übermitteln. Dies ist nicht der Fall. Eine solche Vorgehensweise bedarf vielmehr der Einwilligung der Betroffenen, da eine Rechtspflicht zur Übermittlung nur gegenüber der öffentlichen Stelle besteht, die rechtlich zur jeweiligen Datenerhebung befugt ist. Eine unmittelbare Übermittlung an einen beauftragten Dienstleister kann daher nur ergänzend angeboten, nicht aber verlangt werden.

4. Polizei, Justiz

4.1
Novellierung des Hessischen Sicherheitsüberprüfungsgesetzes (HSÜG) – jetzt: Sicherheitsüberprüfungs- und Verschlusssachengesetz (HSÜVG)

Das Hessische Sicherheitsüberprüfungsgesetz (HSÜG) ist im Jahr 2019 novelliert worden (durch Gesetz vom 11. Dezember 2019, GVBl. S. 406) und nennt sich jetzt Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz (HSÜVG). Im Rahmen der öffentlichen Anhörung im Innenausschuss des Hessischen Landtages habe ich zum Gesetzentwurf eine Stellungnahme abgegeben (Ausschussvorlage INA 20/10, S. 13 ff., zum Gesetzentwurf zur Änderung des Hessischen Sicherheitsüberprüfungsgesetzes, LT-Drs. 20/1090), in der ich verschiedene datenschutzrechtliche Bedenken geäußert habe. Diese Kritikpunkte wurden jedoch vom Gesetzgeber nicht aufgegriffen.

Neben den bereits bei den Beratungen zur vorherigen Fassung des Sicherheitsüberprüfungsgesetzes geäußerten Bedenken zur Einholung einer Schufa-Eigenauskunft (nunmehr in § 10 Abs. 1a Satz 1 HSÜVG), die noch immer relevant sind, habe ich im Rahmen dieses Gesetzgebungsverfahrens im Hinblick auf die Sicherheitsüberprüfung u. a. Kritik an der Ausweitung der Einsicht in Internetseiten und den öffentlich sichtbaren Teil sozialer Netzwerke auf einbezogene Personen (§ 10 Abs. 1a Satz 3, § 11 Abs. 2 i. V. m. Abs. 1 Satz 1 Nr. 17 HSÜVG) geäußert. Insbesondere fehlt es an einer belastbaren Begründung für die Ausweitung auf diesen Personenkreis (in § 3 Abs. 3 Satz 1 HSÜVG sind einbezogene Personen näher definiert). Zudem sind weder aus der als Kann-Vorschrift formulierten Regelung noch aus der Begründung zu § 10 Abs. 1a Satz 3 HSÜVG belastbare Kriterien ersichtlich, wann von der Einsicht abgesehen werden soll. In der Begründung zum Gesetzentwurf (LT-Drs. 20/1090, S. 14) wird lediglich ausgeführt, dass die Ausgestaltung als Kann-Vorschrift der Berücksichtigung des individuellen Bedarfs und der Kapazitäten beim Überprüfungspersonal dienen soll.

§ 3 HSÜVG

(…)

(3) In die Sicherheitsüberprüfung nach den §§ 8 und 9 (Ü2 und 3) sollen einbezogen werden:

1. *die volljährige Ehegattin oder der volljährige Ehegatte der betroffenen Person oder*
2. *die volljährige Lebenspartnerin oder der volljährige Lebenspartner der betroffenen Person und*
3. *die volljährige Person, mit der die betroffene Person in einer auf Dauer angelegten eheähnlichen oder gleichgeschlechtlichen Gemeinschaft lebt (Lebensgemeinschaft).*

(…)

§ 10 HSÜVG

(…)

(1a) Die mitwirkende Behörde kann zusätzlich eine Datenübersicht der Schufa Holding AG nach Art. 15 Abs. 1 der Verordnung (EU) 2016/679 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) bei der betroffenen Person anfordern, wenn Hinweise auf eine mögliche finanzielle Angreifbarkeit bestehen. Bei Personen im Sinne des § 5 Abs. 1 Satz 1 Nr. 3 ist diese Datenübersicht in jedem Fall anzufordern. Die mitwirkende Behörde kann darüber hinaus zu der betroffenen Person in erforderlichem Maße Einsicht in allgemein zugängliche eigene Internetseiten und den öffentlich sichtbaren Teil sozialer Netzwerke nehmen; bei Sicherheitsüberprüfungen nach den §§ 8 und 9 (Ü 2 und 3) kann diese Einsicht auch zu der einbezogenen Person erfolgen. […]

(…)

§ 11 HSÜVG

(1) In der Sicherheitserklärung sind von der betroffenen Person anzugeben:

(…)

Nr. 17 Adresse einer allgemein zugänglichen eigenen Internetseite, Benutzernamen oder ID bei öffentlichen Mitgliedschaften und Teilnahme in sozialen Netzwerken,

(…)

(2) Werden Personen nach § 3 Abs. 3 Satz 1 einbezogen, sind zusätzlich deren in Abs. 1 Satz 1 Nr. 5 bis 7, 11, 14 bis 17 und 20 genannte Daten mit Ausnahme der Anzahl der Kinder anzugeben.

(…)

Des Weiteren habe ich meine Bedenken gegen die neue Vorschrift § 32a HSÜVG vorgetragen, welche die Anwendung des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) und die Befugnisse des Hessischen Beauftragten für Datenschutz und Informationsfreiheit beschränkt

sowie datenschutzrechtliche Sonderregelungen im Bereich der Sicherheitsüberprüfungen schafft.

§ 32a HSÜVG

(1) Für die Anwendung der Vorschriften des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gilt Folgendes:

1. *§ 1 Abs. 8, § 14 Abs. 1 und 3 bis 5 und § 19 finden keine Anwendung,*
2. *die §§ 37, 41, 46 Abs. 1 bis 4 sowie die §§ 47, 48, 49 Abs. 1 und 2, 57, 59 und 78 sind entsprechend anzuwenden.*

(2) Jede Person kann sich an die Hessische Beauftragte oder den Hessischen Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten nach diesem Gesetz durch öffentliche oder nicht öffentliche Stellen in ihren Rechten verletzt worden zu sein.

(3) Die oder der Hessische Beauftragte für Datenschutz und Informationsfreiheit überwacht bei öffentlichen und nicht öffentlichen Stellen die Einhaltung der anzuwendenden Vorschriften über den Datenschutz bei der Erfüllung der Aufgaben dieses Gesetzes. Der Kontrolle durch die Hessische Beauftragte oder den Hessischen Beauftragten für Datenschutz und Informationsfreiheit unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn die betroffene Person der Kontrolle der auf sie bezogenen Daten im Einzelfall gegenüber der oder dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit widerspricht.

(4) Die öffentlichen und nicht öffentlichen Stellen sind verpflichtet, die Hessische Beauftragte oder den Hessischen Beauftragten für Datenschutz und Informationssicherheit bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihr oder ihm ist dabei insbesondere

1. *Auskunft zu seinen oder ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme zu gewähren, die im Zusammenhang mit der Kontrolle nach Abs. 2 stehen,*
2. *jederzeit Zutritt in alle Diensträume zu gewähren.*

Dies gilt nicht, soweit die zuständige oberste Landesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

Insbesondere ist nicht nachvollziehbar, warum die Untersuchungsbefugnisse des Hessischen Beauftragten für Datenschutz und Informationsfreiheit etwa in Abs. 3 Satz 2 (Widerspruchsrecht der betroffenen Person) und in Abs. 4 Satz 3 (Ausschluss der Untersuchungsbefugnisse im Einzelfall durch die zuständige oberste Landesbehörde) derart eingeschränkt sowie die Abhilfebefugnisse auf die Beanstandung und Warnung nach § 14 Abs. 2 HDSIG beschränkt werden, Abs. 1 Nr. 1. Bei der Einschränkung der Untersuchungsbefugnisse handelt es sich maßgeblich um die Übernahme von Regelungen aus dem § 24 Abs. 2 und 4 BDSG alter Fassung (vgl. BT-Drs. 18/11325, S. 126). Diese Regelungen waren auch zu Zeiten der Gültigkeit des BDSG a. F. nicht ohne Kritik (z. B. Dammann in Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014,

§ 24 Rn. 25 ff., 39 ff. mit Nachweisen) und sind vorliegend im Hinblick auf den Ausschluss der Untersuchungsbefugnisse im Einzelfall in Abs. 4 Satz 3 zudem noch verschärft worden (in § 24 Abs. 4 BDSG a. F. galt der Ausschluss etwa nicht für die allgemeine Unterstützungspflicht in Abs. 4 Satz 1).

Im Ergebnis fehlt es an einer tragfähigen Begründung, warum derartige Ein- und Beschränkungen der Befugnisse des Hessischen Beauftragten für Datenschutz und Informationsfreiheit hier notwendig sind. Gerade in diesem sensiblen und wichtigen Bereich der Sicherheitsüberprüfungen sollte eine unabhängige Aufsichtsbehörde als eine mit wirksamen Befugnissen ausgestattete Datenschutzkontrollinstanz agieren können.

4.2
Datenschutzrechtliche Prüfungen im Polizeibereich

Neben der turnusmäßigen Prüfung der Antiterrordatei (ATD) erfolgten 2020 erstmals datenschutzrechtliche Prüfungen meiner Behörde bei der Hessischen Polizei zur Erfüllung meiner neuen gesetzlichen Prüfpflichten.

Im Zuge der Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) im Jahr 2018 sind auch neue datenschutzrechtliche Prüfpflichten für meine Behörde hinzugekommen. Diese neuen Pflichten zur Datenschutzkontrolle ergeben sich konkret aus § 29a HSOG und gelten für präventivpolizeiliche Maßnahmen gemäß dem Katalog in § 28 Abs. 2 HSOG. Um den gesetzlichen Vorgaben bezüglich der neuen Prüfpflichten gerecht zu werden, wurde das zuständige Fachreferat mit einer zusätzlichen Stelle ausgestattet.

§ 28 HSOG

(…)

(2) Zu protokollieren sind je nach Durchführung der konkreten Maßnahme auch bei

1. *Maßnahmen nach § 15 Abs. 2 und 6, bei denen Vorgänge außerhalb von Wohnungen erfasst wurden, die Zielperson und die erheblich mitbetroffenen Personen,*
2. *Maßnahmen nach § 15 Abs. 4 die Person, gegen die sich die Maßnahme richtete, sonstige überwachte Personen und die Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,*
3. *Maßnahmen nach § 15 Abs. 6, bei denen Vorgänge innerhalb von Wohnungen erfasst wurden, und nach § 16 die Zielperson, die erheblich mitbetroffenen Personen und die Personen, deren nicht allgemein zugängliche Wohnung betreten wurde,*

4. Maßnahmen nach § 15a Abs. 1, 2 Satz 1, Abs. 2a Satz 1 und 2 sowie Abs. 3 die Beteiligten der überwachten und betroffenen Telekommunikation, die Nutzerin oder der Nutzer sowie die Zielperson,

5. Maßnahmen nach § 15b die Beteiligten der überwachten Telekommunikation und die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

6. Maßnahmen nach § 15c die Zielperson, die mitbetroffenen Personen und die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

7. Maßnahmen nach § 17 die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind,

8. Maßnahmen nach § 26 die im Übermittlungsersuchen nach § 26 Abs. 2 enthaltenen Merkmale und die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden.

(…)

§ 29a HSOG

Die oder der Hessische Datenschutzbeauftragte führt unbeschadet ihrer oder seiner sonstigen Aufgaben und Kontrollen mindestens alle zwei Jahre zumindest stichprobenartig Kontrollen bezüglich der Datenverarbeitung bei nach § 28 Abs. 2 zu protokollierenden Maßnahmen und von Übermittlungen nach § 23 durch.

Zur Prüfung wurden mir auf Anforderung die Akten zu den Vorgängen vorgelegt, die von mir zuvor für die stichprobenartige Kontrolle zweier Polizeipräsidien ausgewählt worden waren. Die Schwerpunkte der einzelnen Prüfungen waren neben den materiell-rechtlichen Voraussetzungen der Maßnahmen jeweils auch die ausgeübten Anordnungskompetenzen, die fristgerechte Beendigung der Maßnahmen sowie die Handhabung der gesetzlich geregelten Benachrichtigungspflicht gemäß § 29 Abs. 5 bis 7 HSOG.

§ 29 HSOG

(1) Die Betroffenen erhalten Information, Benachrichtigung oder Auskunft hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt, und im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und der Art. 13 bis 15 der Verordnung (EU) Nr. 2016/679, soweit in den Abs. 2 bis 7 nichts Abweichendes geregelt ist.

(…)

(5) Wurden personenbezogene Daten durch Maßnahmen nach § 28 Abs. 2 erlangt, sind die dort jeweils bezeichneten betroffenen Personen hierüber nach Abschluss der Maßnahme zu benachrichtigen. Nachforschungen zur Feststellung der Identität oder zur Anschrift einer zu benachrichtigenden Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(6) Eine Benachrichtigung nach Abs. 5 ist zurückzustellen, solange sie

1. *den Zweck der Maßnahme,*
2. *ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren,*
3. *den Bestand des Staates,*
4. *Leib, Leben oder Freiheit einer Person oder*
5. *Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, gefährden würde. Im Falle des Einsatzes einer V-Person oder VE-Person erfolgt die Benachrichtigung erst, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung der V-Person oder VE-Person möglich ist. Die Entscheidung über das Zurückstellen einer Benachrichtigung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren. Über die Zurückstellung der Benachrichtigung ist die oder der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss der Maßnahme und danach in halbjährlichen Abständen in Kenntnis zu setzen.*

(7) Eine Benachrichtigung nach Abs. 5 unterbleibt, soweit dies im überwiegenden Interesse einer betroffenen Person liegt. Zudem kann die Benachrichtigung einer in § 28 Abs. 2 Nr. 4 und 5 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung hat. Die Entscheidung über das Unterbleiben einer Benachrichtigung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(…)

Im Rahmen der Prüfung habe ich in Bezug auf den Umfang der Benachrichtigungen festgestellt, dass die Benachrichtigungen nach Abschluss der Maßnahmen i. S. d. § 28 Abs. 2 HSOG teilweise nicht in ausreichendem Umfang erfolgten und den inhaltlichen Anforderungen nicht immer genügten. Auch für Benachrichtigungen nach § 29 Abs. 5 HSOG gilt § 29 Abs. 1 HSOG, der auf die Regelungen zu den Betroffenenrechten, wie die vorliegend insbesondere einschlägige Vorschrift des § 51 HDSIG, verweist. Hier habe ich veranlasst, dass neue Muster erarbeitet werden, die dann künftig im Rahmen der Benachrichtigung der betroffenen Personen genutzt werden sollen.

Zudem habe ich erkannt, dass die Dokumentation der prüfungsrelevanten Inhalte in den Akten für datenschutzrechtliche Prüfzwecke noch zu verbessern ist. Darauf wurden die betreffenden Stellen von mir hingewiesen.

Die Auswertung der Prüfung ist allerdings noch nicht vollständig abgeschlossen.

Des Weiteren wurde im Jahr 2020 erneut die Antiterrordatei von mir geprüft. Die Prüfungen erstreckten sich auf ausgewählte Polizeipräsidien und das Landesamt für Verfassungsschutz Hessen. Gegenstand der diesjährigen Prüfung waren die im Jahr 2019 neu angelegten Datensätze. Die Kontrolle ergab keine fehlerhaften Datenverarbeitungen oder sonstige Auffälligkeiten. Positiv festzustellen war, dass die Aktenführung bei der Polizei und dem Landesamt für Verfassungsschutz Hessen mittlerweile gemäß unseren Vorschlägen aus vergangenen Prüfungen angepasst wurde und die Akten für die datenschutzrechtlichen Prüfungszwecke nunmehr besser strukturiert sind.

5. Schulen, Hochschulen

5.1
Dokumentation zur Befreiung vom Tragen des Mund-Nasen-Schutzes in der Schule

Die Schulen sind durch die Corona-Pandemie vielfältig gefordert. Das betrifft auch den Umgang mit Schülerinnen und Schülern, die durch ein ärztliches Attest von der Verpflichtung zum Tragen eines Mund-Nasen-Schutzes befreit worden sind. Hinsichtlich der Dokumentation der Befreiung vertrete ich die Auffassung, dass ein Vermerk in der Schülerakte über die Vorlage des Attests ausreicht. Auch halte ich die Nennung einer Diagnose für nicht erforderlich. Das Hessische Kultusministerium hat sich dem angeschlossen und die Schulen darüber informiert.

Aus dem Bereich des Staatlichen Schulamtes (SSA) für den Landkreis und die Stadt Kassel erreichten mich die ersten Beschwerden von Eltern darüber, dass Schulen ärztliche Atteste über die Befreiung vom Tragen des Mund-Nasen-Schutzes in der Schule kopierten und in der Schülerakte ablegten oder auch die Nennung einer Diagnose im Attest einforderten. Dabei beriefen sich die betroffenen Schulen auf eine Handlungsanleitung des dortigen SSA.

Gerichte halten Diagnose im Attest und Verortung in der Schülerakte für rechtmäßig

Die Handlungsanleitung für die Schulen hatte das SSA für den Landkreis und die Stadt Kassel auf Grundlage eines Beschlusses des Verwaltungsgerichts (VG) Würzburg (Az.: W 8 E.10.1301 vom 16.09.2020) kommuniziert. Die Verwaltungsrichter erachteten es ebenso als verpflichtend, eine Kopie des ärztlichen Attestes als Nachweis in die Schülerakte aufzunehmen wie auch die Nennung einer Diagnose im Attest. Diese Rechtsauffassung teilten eine Reihe weitere Verwaltungsgerichte in anderen Bundesländern. Zudem gab es zwei Beschlüsse von Oberverwaltungsgerichten (OVG Münster vom 24.09.2020, Az.: 13 B 1368/20 und VGH München vom 26.10.2020, Az.: 20 CE 20.2185) gleichlautenden Inhalts.

Meine Rechtsauffassung wird vom Hessischen Kultusministerium geteilt

Ich selbst und teilweise auch andere Datenschutz-Aufsichtsbehörden sind jedoch entgegen der bisherigen Rechtsprechung anderer Auffassung:

Die Rechtsgrundlage für die Verpflichtung zum Tragen eines Mund-Nasen-Schutzes ergibt sich aus dem Infektionsschutzgesetz sowie der jeweils aktuellen Landesverordnung zur Bekämpfung des Corona-Virus. Darin wird zum Ausdruck gebracht, dass die Befreiung durch die Betroffenen glaubhaft zu machen ist. Dies erfolgt durch die Vorlage eines Attestes. Im Gegensatz zu den bisher bekannten gerichtlichen Entscheidungen erachte ich die Nennung einer Diagnose weder für zwingend noch erforderlich. Schulleitung und Lehrkräfte vermögen in der Regel aufgrund mangelnder medizinischer Kenntnisse keine Bewertung der Diagnosen vorzunehmen. Dies ist auch nicht erforderlich, weil dies nicht zur Aufgabenstellung einer Schule zählt. Außerdem ist dem Grundsatz der Datensparsamkeit i. S. v. Art.5 Abs. 1 lit. c Rechnung zu tragen. Zudem handelt es sich um Gesundheitsdaten und damit um Daten einer besonderen Kategorie im Sinne von Art. 9 Abs. 1 DS-GVO. Dass deren Verarbeitung in diesem konkreten Fall durch ein bestehendes öffentliches Interesse (§ 9 Abs. 2 lit. c DS-GVO) gerechtfertigt werden könnte, vermag ich so nicht nachzuvollziehen.

Ebenfalls als unverhältnismäßig erachte ich, eine Kopie des ärztlichen Attestes in der Schülerakte zu verorten. Selbstverständlich muss der Schule die Möglichkeit gegeben werden, das Original des Attestes in angemessener Form einsehen zu können. Sofern im konkreten Einzelfall seitens der Schule Zweifel an der Echtheit eines ärztlichen Attestes bestehen sollten, ist das weitere Vorgehen mit dem Staatlichen Schulamt abzustimmen. Die Vorlage des Attestes wird mit Angabe des ausstellenden Arztes oder der Ärztin dokumentiert. Eine Vorlage hierfür hat das HKM mit Schreiben vom 21.09.2020 den Schulen ebenso zur Verfügung gestellt wie eine allgemeine Handlungsanleitung zum Umgang mit ärztlichen Attesten.

Die schnelle Abstimmung mit dem HKM hat dazu geführt, dass es in Hessen zu keiner mir bekannten verwaltungsgerichtlichen Entscheidung kommen musste, die das Thema Mund-Nasen-Schutz zur Grundlage hatte. Die Schulen haben sich offensichtlich an die Vorgaben gehalten, so dass wenige Wochen nach den ersten Beschwerden keine weiteren Fälle an mich herangetragen wurden.

5.2
Einsatz von Videokonferenzsystemen in Schulen

Der Einsatz von Videokonferenzsystemen in Schulen wirft datenschutzrechtliche Fragen auf. Im Frühjahr vergangenen Jahres habe ich im Rahmen des ersten Lock-Downs für die pädagogische Nutzung eine weitgehende Duldung fast aller Systeme ausgesprochen, die ich im August 2020 mit bestimmten Auflagen versehen bis zum 31. Juli 2021 verlängert habe. Bis zu diesem Zeitpunkt soll das Hessische Kultusministerium ein landesweites Angebot für seine Schulen realisiert haben.

Schulschließungen erfordern ein schnelles Handeln

Bis zum Beginn des ersten Lock-Downs im März 2020 war der Einsatz von Videokonferenzsystemen (VKS) für Schulen kein Thema, da damals in einem festgelegten Rahmen der Unterricht in Präsenzform stattfand. Erst mit den staatlichen Verfügungen, wegen der Pandemie u. a. auch die Schulen zu schließen, mussten Überlegungen angestellt werden, den Kontakt der Schule mit den Schülerinnen und Schülern auf geeignete Weise aufrechtzuerhalten, um zumindest u. a. Aufgaben übermitteln zu können. In aller Eile wurde nun nach geeigneten VKS gesucht, wobei Überlegungen hinsichtlich des Datenschutzes in vielen Fällen nicht an vorderer Stelle standen.

Das Hessische Kultusministerium (HKM) trat an mich heran und erbat in Anbetracht der Eilbedürftigkeit in der Sache und wegen der mangelnden Kenntnisse vieler Schulleitungen rund um die Datenverarbeitung bei der Nutzung von VKS um eine pragmatisch orientierte Freigabe der Produkte. Die Sicherstellung des schulischen Bildungs- und Erziehungsauftrages gepaart mit einer gänzlich unbekannten Situation rund um die pandemische Entwicklung haben mich dann dazu bewogen, für den Einsatz digitaler Werkzeuge temporär das Datenschutzniveau zu senken (s. a. Homepage des HBDI, Beitrag vom 23. März 2020 – *https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/informationen-zum-digitalen-lernen-und-der-digitalen*). Zudem hatte ich eine bis August 2020 befristete Duldung fast aller VKS-Systeme für den pädagogischen Bereich auf der Grundlage von Art. 6 Abs. 1 lit. d und e ausgesprochen. Bewusst habe ich darauf verzichtet, durch stringente Vorgaben die unvorhersehbare Situation für die Schulen durch komplexe datenschutzrechtliche Vorgaben noch schwieriger werden zu lassen. Dabei war ich mir darüber im Klaren, dass insbesondere der Einsatz US-amerikanischer Produkte konfliktbehaftet sein könnte, da über deren Datenschutzkonformität keine Aussagen getroffen werden konnten. Zwar gab es in der Tat auch kritische Stimmen aus der Lehrer- und Elternschaft.

Insgesamt sehe ich mich aber mit in meiner Einschätzung und den daraus abgeleiteten Handlungsvorgaben bestätigt.

Duldung wird mit Auflagen verlängert

Das von mir geforderte datenschutzkonforme, landesweite Angebot für die Schulen, welches das HKM zur Verfügung gestellt hat und auf der Open-Source-Software BigBlueButton basiert, konnte bis zum Beginn des neuen Schuljahres nicht realisiert werden. Deshalb trat das Ministerium erneut an mich heran und bat um die Verlängerung der Duldungsphase. Dieser Bitte habe ich entsprochen und die Duldung bis zum 31. Juli 2021 verlängert. Allerdings habe ich an die Verlängerung Bedingungen geknüpft (zu den Einzelheiten s. a. Homepage des HBDI – *https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/hbdi-duldet-%C3%BCbergangsweise-den-einsatz-von*).

Das HKM ist nun gefordert, im Rahmen einer europaweiten Ausschreibung ein VKS auf der Basis der Open-Source-Anwendung BigBlueButton (BBB) zu etablieren, das an dem Hessischen Schulportal angedockt werden soll. Deshalb ist davon auszugehen, dass die Schulen in Hessen ab dem Schuljahr 2021/22 über ein datenschutzkonformes VKS verfügen werden. Meine Unterstützung bei der Umsetzung der datenschutzrechtlichen Erfordernisse habe ich zugesagt.

Eine Digitalisierungsnorm tut schon lange Not

Wiederholt habe ich das HKM in der Vergangenheit darauf aufmerksam gemacht, dass eine Rechtsgrundlage für den Einsatz digitaler Werkzeuge durch die Schule dringend geboten ist. Leider hat man meine Hinweise bislang nicht umgesetzt und das Hessische Schulgesetz nicht um eine Digitalisierungsnorm ergänzt. Schule muss aber im Rahmen ihres pädagogischen Handlungsspielraumes in die Lage versetzt werden, auf Grundlage eines Beschlusses der Schul- oder Lehrerkonferenz ihren an den eigenen Bedarfen orientierten Weg in die Digitalisierung zu beschreiten. Sind die rechtlichen und organisatorischen Voraussetzungen hierfür geschaffen, ist die Einholung der Einwilligung bei Schülerinnen und Schülern oder den Eltern, die bislang zwingend ist, dann nicht mehr erforderlich. Allerdings muss die Schule die Datensicherheit sowie die Teilhabe aller Betroffenen gewährleisten.

5.3
Dienstliche E-Mail-Adressen für Lehrkräfte

Einer von mir seit Jahren gestellten Forderung zur Verbesserung des Datenschutzes im schulischen Bereich ist das Hessische Kultusministerium (HKM) im Berichtsjahr nachgekommen. Die Einführung dienstlicher E-Mail-Adressen für die hessischen Lehrkräfte verbessert deren Arbeitssituation maßgeblich und macht deren Datenverarbeitung sicherer.

Ein dienstlicher E-Mail-Account, der mit dem Namen des oder der Betroffenen beginnt, ist in fast allen Bereichen der öffentlichen Verwaltung etabliert. Seither davon ausgenommen waren die Lehrkräfte. Möglicherweise war dies der besonderen Arbeitssituation der Lehrkräfte geschuldet, die über keinen Arbeitsplatz im herkömmlichen Sinn verfügen und wesentliche Tätigkeiten, wie z. B. die Unterrichtsvorbereitung oder Korrektur von Klausuren, im häuslichen Bereich ausüben. Jedenfalls war der dienstliche E-Mail-Account über viele Jahre hinweg und trotz meiner wiederholten Interventionen für das HKM kein Thema. Deshalb waren es zum Teil Schulträger, die den Beschäftigten schulbezogene E-Mail-Accounts zur Verfügung stellten oder die Schulen richteten selbst über einen Provider E-Mail-Adressen für die Lehrkräfte ein. In nicht wenigen Fällen wurde aber auch der private E-Mail-Account genutzt: Die Vermischung von privaten und dienstlichen E-Mails war damit unvermeidbar und beinhaltete datenschutzrechtliches Risikopotenzial.

Prozess der technischen Umsetzung ist anspruchsvoll

Ein derartiges Projekt, nämlich annähernd 70.000 E-Mail-Adressen einzurichten, ist technisch und organisatorisch enorm aufwändig. Obwohl von meiner Seite aus nicht gefordert, beauftragte das HKM den staatlichen Dienstleister Hessische Zentrale für Datenverarbeitung (HZD) mit der Umsetzung des Projekts. Zusätzlich erforderliche personelle Ressourcen wurden vom Ministerium bereitgestellt.

In einer kurzen Zusammenfassung lässt sich das Verfahren zur Erstellung eines dienstlichen E-Mail-Accounts wie folgt beschreiben:

Wird eine Lehrkraft neu eingestellt, teilt diese im Arbeitsvertrag ihre persönlichen Daten mit. Mit der Übergabe des Arbeitsvertrags wird der Einstellungsprozess in der Personalverwaltung angestoßen, bei dem ein zuständiger Mitarbeiter die hinterlegten Informationen teils manuell als Stammdatensatz in die Personaldatenbank des Landes Hessen (SAP HR) aufnimmt. Der Stammdatensatz bildet die Grundlage für die digitale Identität des Mitarbeiters und verfügt mit der Personalnummer über ein eindeutiges Identitätsmerkmal

(Unique Identifier), anhand dessen die neue Lehrkraft zukünftig zweifelsfrei identifiziert werden kann.

Danach legt das Datenintegrationssystem ein neues Benutzerkonto für die Lehrkraft in der Benutzerverwaltung (Schul-Active-Directory) an, das u. a. als Grundlage für die spätere Authentifizierung der Lehrkraft dient, sobald diese sich über die URL an ihrem Postfach anmeldet.

In der Postfachumgebung legt das Datenintegrationssystem ein deaktiviertes RAD-Konto (Ressource Active Directory Konto) und ein verknüpftes Postfach an, das mit einem bestimmten Konto in der Benutzerverwaltung verlinkt wird.

Auf diese Weise wird sichergestellt, dass die Lehrkraft bei der Anmeldung gegen ihr Konto authentifiziert und mit ihrem E-Mail-Postfach verbunden wird. Sobald die Informationen in der Benutzerverwaltung und in der Postfachumgebung umgesetzt wurden, wird die neue E-Mail-Adresse, die einer zentralen Namenskonvention folgt, mit dem Benutzerkonto durch das Datenintegrationssystem synchronisiert. Anschließend werden der neuen Lehrkraft die Daten ihres Postfachs inklusive des initialen Kennworts mitgeteilt.

Die Beschreibung betrifft nur die Fallkonstellation „Neueinstellung einer Lehrkraft“. Ähnlich komplexe Schritte müssen für bereits eingestellte Lehrkräfte vollzogen werden, aber auch für den Fall der Namensänderung oder des Ausscheidens aus dem Dienst. Mit Hilfe einer Zwei-Faktor-Authentisierung kann die Lehrkraft die Freischaltung ihres Postfaches vornehmen. Hierzu müssen allerdings die privaten Endgeräte ebenso eingesetzt werden wie für die Nutzung des Postfachs.

Nutzungsrichtlinie definiert Rechte und Pflichten

Eine vom Ministerium erarbeitete Nutzungsrichtlinie konkretisiert die Handhabung der dienstlichen E-Mail-Accounts. So wird zunächst festgestellt, dass die Nutzung durch die Lehrkräfte im dienstlichen Kontext verpflichtend ist. Auch ist ein regelmäßiger Abruf und damit die Kenntnisnahme eingehender E-Mails festgelegt. Die Nutzung privater Endgeräte der Lehrkraft ist grundsätzlich unter bestimmten technischen Voraussetzungen erlaubt. Unberührt hiervon bleibt jedoch die generelle datenschutzrechtliche Problematik um das sogenannte Bring Your Own Device (BYOD), also der Nutzung privater Endgeräte für den dienstlichen Bereich. Möglicherweise werden der Digitalpakt und das Vorhaben, Lehrkräfte mit dienstlichen Endgeräten auszustatten, auch dieses datenschutzrechtliche Defizit beseitigen.

Die Speicherung und Übermittlung personenbezogener Daten über die dienstliche E-Mail-Adresse ist nur unter Beachtung der für Schulen geltenden datenschutzrechtlichen Regelungen zulässig. Sie darf nur im Rahmen der dienstlichen Aufgabenstellung erfolgen, soweit es für den dabei jeweils verfolgten dienstlichen Zweck erforderlich ist. Besonders sensible personenbezogene Daten nach Art. 9 DS-GVO dürfen nicht als Inhalt oder Anhang einer E-Mail verschickt werden, soweit diese nicht verschlüsselt sind.

Das betrifft Angaben über die Gesundheit, Behinderung, also auch Daten bezüglich sonderpädagogischer Förderung, Herkunft, Religion, politische oder weltanschauliche Überzeugungen, sexuelle Orientierung, Gewerkschaftszugehörigkeit. Dasselbe gilt für Personalaktendaten und andere personenbezogene Daten, die einem hohen Schutzbedarf unterliegen. Werden für die Nutzung der dienstlichen E-Mail-Adresse unter den in Nr. 8 dieser Richtlinie genannten Voraussetzungen private Endgeräte verwendet, dürfen darauf nach § 83 Abs. 1 und Abs. 7 HSchG und § 1 Abs. 5 und § 3 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen nur die in Anlage 1 Abschn. A 6 genannten personenbezogenen Daten von Schülerinnen und Schülern und deren Eltern verarbeitet werden. Daten mit einem normalen Schutzbedarf können demnach mit der dienstlichen E-Mail-Adresse kommuniziert werden.

In der Richtlinie wird weiterhin ausgeführt, dass eine Auswertung der angefallenen Protokolldaten aus Gründen der Daten- und Systemsicherheit, der Systemtechnik (z. B. zur Fehlerbehebung und -verfolgung) und zur Missbrauchskontrolle erfolgt. Die Auswertungen finden anlassbezogen statt. Die Abfrage und Auswertung der Daten erfolgt durch das Hessische Kultusministerium beispielsweise dann, wenn der Verdacht besteht, dass ein Zugang für unbefugte Dritte besteht („Hacking“). Die Auswertung kann im konkreten Verdachtsfall außerdem auf Anordnung der Dienststellenleitung erfolgen. Die Personalvertretung und die behördlichen Datenschutzbeauftragten sind in diesem Fall zu beteiligen. Darüber hinaus ist eine Auswertung mit Zustimmung der oder des Betroffenen jederzeit möglich. Der Grund für die Auswertung und deren Ergebnis ist nachvollziehbar zu dokumentieren.

Ergänzungen, die ich für erforderlich gehalten hatte, wurden vom Ministerium in die Richtlinie übernommen. Bis zum Februar 2021 sollte der Prozess zur Einführung der dienstlichen E-Mail-Adresse für Lehrkräfte abgeschlossen sein.

6. Verkehrswesen

6.1
Datenschutzvorfall beim Dienstleister von Verkehrsverbünden

Kundendaten aus den sogenannten Sperrlisten der Verkehrsverbünde waren im Internet abrufbar – Datenleck geschlossen, erforderliche technisch-organisatorische Maßnahmen ergriffen und betroffene Personen informiert.

Im Berichtszeitraum wurde mir eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO von mehreren Verkehrsverbünden gemeldet. Auch andere Datenschutzaufsichtsbehörden wurden von bundesländerübergreifend tätigen Verkehrsverbünden informiert. Hintergrund der Meldungen war eine unbeabsichtigte Veröffentlichung von personenbezogenen Daten im Internet in Bezug auf sogenannte Sperrlisten. Bei diesen zum Mobile-Ticketing-System gehörigen Sperrlisten handelt es sich um die Fahrgastdaten im Zusammenhang mit der Sperrung von Nutzeraccounts. Die Sperrung eines Nutzeraccounts kann bspw. die Folge eines erfolglosen Mahnvorgangs bei der Nichtzahlung gekaufter Tickets sein. Die Sperrung des Nutzeraccounts verhindert den Erwerb von Tickets und die Neuanmeldung mit denselben Daten.

Die Kundendaten waren durch einen Konfigurationsfehler eines Dienstleisters (Auftragsverarbeiters) mehrere Jahre lang über das Internet unter einer nicht öffentlich bekannten Webadresse ohne Zugriffsschutz abrufbar. Die Webadresse war jedoch nicht mit gängigen Suchmaschinen auffindbar.

Der Dienstleister hat den Fehler selbst entdeckt und die verantwortlichen Verkehrsverbünde entsprechend informiert. Als direkte Reaktion auf die Identifikation des Vorfalls wurde die Zugriffsmöglichkeit über das Internet deaktiviert und die unmittelbare Verletzung des Schutzes personenbezogener Daten damit abgestellt.

Ob das Datenleck tatsächlich durch unberechtigte Zugriffe ausgenutzt wurde, konnte nicht für die gesamte Zeit der Exposition geklärt werden, konnte aber auch nicht ausgeschlossen werden. Die vom Dienstleister vorgenommene Analyse der verfügbaren Logdaten hat jedoch keine Anzeichen für Zugriffe Dritter ergeben. Auch konnten keine sonstigen Indizien für eine missbräuchliche Verwendung der personenbezogenen Daten identifiziert werden.

Als Reaktion auf die Meldung haben meine Mitarbeiter weiterführende technische Prüfungen vorgenommen. Die hierbei gewonnenen Erkenntnisse wurden den Verantwortlichen zusammen mit den aufgetretenen Fragestellungen mitgeteilt, und sie wurden zu einer Stellungnahme aufgefordert.

In der Folge kam es zu einem umfangreichen Informationsaustausch zwischen den Verantwortlichen und dem Auftragsverarbeiter auf der einen und meinen Mitarbeitern auf der anderen Seite. Hierbei wurden über die eigentliche Verletzung hinausgehende Fragestellungen hinsichtlich der zugrundeliegenden IT-Infrastruktur, der zugehörigen IT-Systeme und der mittels dieser umgesetzten IT-Dienste erörtert. Darüber hinaus wurden die zugehörigen Entwicklungs-, Betriebs- und Wartungsprozesse in die Betrachtungen mit einbezogen.

Im Laufe der Sachverhaltsklärung stellte sich heraus, dass ein Projekt zur umfassenden Überarbeitung und Verbesserung der Prozesse bereits vor der Identifikation der Verletzungen des Schutzes personenbezogener Daten initiiert worden war. Insofern war die Identifikation der Verletzungen des Schutzes personenbezogener Daten nicht Ursache, sondern Folge des angestoßenen Projektes. Eine Verbesserung des Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluation der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d DS-GVO lag ebenfalls im Fokus des Projekts. Dieses Projekt war im Zeitraum meiner Prüfungen noch nicht abgeschlossen. Der geplante weitere Projektverlauf wurde mir in Form einer Roadmap dargestellt und im Rahmen eines Termins mit allen Beteiligten erläutert.

Neben der Behebung der Verletzungen des Schutzes personenbezogener Daten konnte ich mich davon überzeugen, dass der von den Verkehrsverbünden und ihrem Auftragsverarbeiter eingeschlagene Weg weit über die konkrete Adressierung der Verletzungen des Schutzes personenbezogener Daten hinausgeht. Die eingeleiteten Maßnahmen erscheinen mir geeignet, um die Sicherheit der Verarbeitung im Sinne des Art. 32 DS-GVO ganzheitlich und umfassend zu verbessern. Ich beabsichtige, mich zu gegebener Zeit von der erfolgreichen Umsetzung der weiteren geplanten Maßnahmen zu überzeugen.

Insgesamt konnte ich feststellen, dass die der Meldung gemäß Art. 33 DS-GVO zugrundeliegenden Verletzungen des Schutzes behoben wurden und dass eine Wiederholung dieser Verletzungen nicht zu erwarten ist.

Die von den Verletzungen des Schutzes personenbezogener Daten betroffenen Personen wurden nach Durchführung der Risikobewertung und nach Inanspruchnahme meiner Beratung durch die Verkehrsverbünde gemäß Art. 34 DS-GVO benachrichtigt, sofern sie identifiziert werden konnten. Zusätzlich veröffentlichten die Verkehrsverbünde eine entsprechende Pressemitteilung.

6.2
Kennzeichenerfassung in öffentlich zugänglichen Parkhäusern

Der Einsatz von Kennzeichenerfassungssystemen in Parkhäusern kann bei Beachtung bestimmter Anforderungen zulässig sein.

Im Jahr 2020 erreichten mich Bürgerbeschwerden, dass vermehrt beim Parken in den öffentlichen Parkhäusern automatisierte Kennzeichenerfassung anstelle des Papierparkscheins eingeführt wird. Diese Vorgehensweise verletze den Datenschutz, denn Parken mit Parkschein sei eine datenschutzschonendere Alternative. Als ein weiteres Argument für die Unzulässigkeit automatisierter Kennzeichenerfassung wurde auch die Rechtsprechung des Bundesverfassungsgerichts (BVerfG Beschl. v. 18.12.2018 – 1 BvR 142/15 (Kfz-Kennzeichenkontrollen 2)) zur automatisierten Kennzeichenkontrolle durch die Polizei vorgetragen.

Bei der automatisierten Kennzeichenerfassung werden Videokameras an der Ein- und Ausfahrt des Parkhauses installiert. Diese Kameras werden mit einer Software betrieben, die das Kfz-Kennzeichen automatisch erkennt und zusammen mit der Einfahrts- und Ausfahrtszeit speichert. Die Fahrerin oder der Fahrer und Insassen werden von der Kamera nicht erfasst. Bei der Ausfahrt wird das erfasste Kennzeichen nach Bezahlung der Parkgebühr erkannt und die Ausfahrtsschranke geöffnet.

Zwischen dem Parkenden und dem Betreiber des Parkhauses wird durch faktisches Verhalten (Parken) ein Einstellvertrag geschlossen. Die Parkdauer bestimmt das zu zahlende Parkentgelt. Die automatisierte Kennzeichenerfassung wird von den Parkhausbetreibern primär zur Erfassung der Parkdauer und zur Vorbeugung von Betrugsfällen bezüglich der Parkdauer eingesetzt. Auch die Einfahrt- und Ausfahrtvorgänge sollen dadurch beschleunigt werden.

Die Verarbeitung von personenbezogenen Daten – ein Kfz-Kennzeichen ist gemäß § 45 S. 2 StVG ein personenbezogenes Datum – ist nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig, wenn sie zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist.

Die Beschwerdeführer stellten sich beim Einsatz der automatisierten Kennzeichenerfassungssysteme auf den Standpunkt, dass die Erforderlichkeit aufgrund eines Alternativverfahrens der Parkdauererfassung mithilfe eines Papierparkscheins zu verneinen wäre.

Welche Datenverarbeitungen zur Erfüllung des Vertrages erforderlich sind, wird primär durch den gegenständlichen Vertragsinhalt und den Vertragszweck bestimmt. Die Parkdauer als Bemessungsgrundlage für die Parkgebühren muss unstrittig erfasst werden. Aber auch die konkrete Erfassungsmethode

muss erforderlich im Sinne dieser Vorschrift sein. Dem Verantwortlichen darf keine mildere, aber gleichermaßen geeignete und zumutbare Erfassungsmethode zur Verfügung stehen. In diesem Zusammenhang muss eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung der Parkenden und dem Interesse des Parkhausbetreibers, ein zeitgemäßes, effizientes und konkurrenzfähiges Produkt anzubieten, stattfinden. Auch der technologische Progress und der neueste Stand der Technik ist in diese Abwägung einzubeziehen, was nicht bedeutet, dass einsatzfähig ist, was technisch möglich ist. Die Verhältnismäßigkeit muss auf jeden Fall gewahrt bleiben.

Das Interesse des Parkhausbetreibers an der Optimierung des Betriebsablaufs, besserer Betrugsprävention, weniger Verwaltungsaufwand und kundenfreundlicherer Abrechnung im Falle des Verlustes des Parkscheins überwiegen das Interesse der Parkenden an der Nichterfassung ihrer Kennzeichen meiner Ansicht allerdings nur dann, wenn das erfasste Kennzeichen nach Beendigung des Parkvorgangs unwiederbringlich gelöscht wird.

Die Unzulässigkeit der Kennzeichenerfassung folgt auch nicht aus der Rechtsprechung des Bundesverfassungsgerichts.

Dort wurde eine Vielzahl der Verkehrsteilnehmer, ohne dass ein konkreter Verdacht gegen diese vorlag, mittels der automatisierten Kennzeichenkontrolle generell und anlassunabhängig mit Fahndungsbestand abgeglichen. Im konkreten Fall findet aber die Kennzeichenerfassung anlassbezogen im Zusammenhang der Erfüllung des Einstellvertrages statt und trifft nur die Parkenden.

In allen mir vorliegenden Fällen habe ich zur Herstellung der Transparenz einen frühzeitigen Hinweis auf die stattfindende Kennzeichenerfassung verlangt. Dies bestimmt sich je nach tatsächlichen Gegebenheiten. Spätestens bei der Einfahrt in die Tiefgarage muss über die automatisierte Kennzeichenerfassung informiert werden. Ein Hinweis erst am Ticketautomaten erfüllt diese Anforderung nicht. Ich empfehle, aufgrund der erschwerten Erkennbarkeit der Hinweisschilder während der Fahrt und der begrenzten Aufnahmefähigkeit aufgrund der Konzentration auf den Verkehr zusätzlich auf der Internetseite des Parkhauses einen entsprechenden Hinweis zu platzieren.

Eine Wendemöglichkeit als unabdingbare Voraussetzung für den Einsatz der Technik wird von mir dagegen nicht verlangt.

Unter der Bedingung der unwiederbringlichen Löschung der erfassten Kennzeichen und des Ergreifens sonstiger, insbesondere durch Art. 32 DS-GVO geforderter Maßnahmen kann der Einsatz automatisierter Kennzeichenerfassung datenschutzkonform gestaltet werden.

6.3
Auskunft über Daten, die nur aufgrund von gesetzlichen Aufbewahrungsfristen vorgehalten werden

Der Ausschluss des Auskunftsrechts in Bezug auf solche personenbezogenen Daten, die einer Aufbewahrungspflicht unterliegen, gilt nicht absolut. Er steht vielmehr unter dem Vorbehalt, dass die Auskunftserteilung einen unverhältnismäßigen Aufwand im konkreten Fall erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

Im Rahmen der Auskunftserteilung nach Art. 15 DS-GVO kam es im Berichtszeitraum vor, dass Verantwortliche personenbezogene Daten, die aufgrund von § 257 HGB vorgehalten wurden, nicht in das Auskunftsschreiben aufgenommen hatten. Begründet wurde dies damit, dass diesbezüglich gemäß § 34 Abs. 1 BDSG eine Befreiung von der Auskunftspflicht bestehe.

Des Weiteren teilte ein Energieversorger im Rahmen der Auskunftserteilung nach Art. 15 DS-GVO allen Auskunftsverlangenden pauschal mit, dass es sein könne, dass weitere personenbezogene Daten aufgrund von gesetzlichen Aufbewahrungsvorschriften gespeichert werden und ihre Auskunftserteilung aufgrund des unverhältnismäßigen Aufwandes verweigert wird.

§ 34 BDSG entbindet die Verantwortlichen von ihrer Auskunftspflicht nach Art. 15 DS-GVO. Die für diesen Tätigkeitsbeitrag relevante Regelungsalternative des Absatzes 1 Nummer 2 a gibt der datenverarbeitenden Stelle die Möglichkeit, die Auskunftserteilung bezüglich der Daten zu verweigern, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen. Allein die Tatsache der Speicherung aufgrund einer Aufbewahrungspflicht führt aber nicht automatisch zur Einschränkung der Auskunftserteilung. Die Erteilung der Auskunft kann nur dann verweigert werden, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und auch technisch-organisatorische Maßnahmen getroffen wurden, die eine Verarbeitung zu anderen Zwecken ausschließen. Gerade diese im zweiten Halbsatz geregelten Anforderungen werden in der Praxis oft nicht beachtet, da irrtümlich davon ausgegangen wird, dass diese nur für die Regelungsalternative des Abs. 1 Nummer 2 b gelten.

Die Beachtung folgender Aspekte im Zusammenhang mit der Auskunftsverweigerung nach § 34 BDSG wurde von mir gefordert:

– Eine gesetzliche oder satzungsmäßige Aufbewahrungsvorschrift verpflichtet den Verantwortlichen, personenbezogene Daten zu speichern. Die gängigsten gesetzlichen Aufbewahrungsvorschriften sind § 257 HGB und § 147 Abs. 3 AO.

Parallel dazu regelt Art. 17 Abs. 3 lit. b DS-GVO (und § 35 Abs. 3 BDSG für vertragliche und satzungsmäßige Aufbewahrungspflichten) im Falle des Vorliegens einer Aufbewahrungsvorschrift eine Ausnahme vom Recht auf Löschung des Betroffenen.

– Die Speicherung von personenbezogenen Daten erfolgt nur auf der Grundlage dieser Aufbewahrungsvorschrift.
  Damit ist die Anwendung dieses Ausnahmetatbestands ausgeschlossen, wenn die Speicherung der Daten auch einem anderen Zweck dient oder die Aufbewahrungsfrist bereits abgelaufen ist.
– Der Verantwortliche stellt einen unverhältnismäßigen Aufwand für die Erteilung der Auskunft fest.
  Dabei muss der Aufwand der konkreten Auskunftserteilung das Informationsinteresse des Auskunftsberechtigten in unverhältnismäßiger Weise überwiegen. Diese Abwägung wird von dem Verantwortlichen grundsätzlich bei jedem Auskunftsverlangen vorgenommen. Bei gleichgelagerten Fällen kann sie einmal erfolgen und muss dann auch nur einmal dokumentiert werden.
  Zugunsten der betroffenen Person sind bei der Ermittlung des Aufwands auch die bestehenden technischen Möglichkeiten zu berücksichtigen, gesperrte und archivierte Daten der betroffenen Person bei der Auskunftserteilung verfügbar zu machen (BT-Drs. 18/11325 S. 104).
  Die Datenschutzaufsichtsbehörde kann das Vorliegen des unverhältnismäßigen Aufwandes vollumfänglich überprüfen.
– Es müssen technisch-organisatorische Maßnahmen vorliegen, welche die Verarbeitung zu einem anderen Zweck ausschließen.
  Welche Maßnahmen im Einzelnen dafür zu ergreifen sind, bestimmt sich nach der Art der gespeicherten Daten und den Umständen der Speicherung. Beispiele für die Maßnahmen ist die Führung von getrennten Datenbeständen (produktiver Datenbestand und gesperrte Aufbewahrungsdaten) und eingeschränkte Zugriffsrechte.
– Die tatsächlichen und rechtlichen Gründe der Auskunftsverweigerung müssen in nachvollziehbarer Weise dokumentiert werden und im Bedarfsfall der Datenschutzaufsichtsbehörde zur Verfügung gestellt werden.
– Der Verantwortliche muss dem Betroffenen die maßgeblichen Gründe für die Auskunftsverweigerung mitteilen, es sei denn, durch die Mitteilung würde der mit der Auskunftsverweigerung verfolgte Zweck gefährdet.

Die auskunftspflichtigen Stellen wurden aufgefordert, die dargestellten Anforderungen zu beachten und ihre Praxis anzupassen.

Der Energieversorger im o. g. Fall wurde aufgefordert, seine Praxis zu ändern und nur denjenigen Auskunftsverlangenden gegenüber die Auskunftsver-

weigerung geltend zu machen, deren Daten tatsächlich aufgrund der Aufbewahrungspflichten vorgehalten werden und bei denen unverhältnismäßiger Aufwand nachweisbar festgestellt werden konnte. Auch wurde er auf seine Begründungspflicht hingewiesen.

7. Beschäftigtendatenschutz, Soziales

7.1
Biometrische Arbeitszeiterfassung mittels Fingerabdruck

Verantwortliche, die ihre Beschäftigten verpflichten, an Systemen teilzunehmen, welche die Zeit mittels Fingerabdrucks erfassen, um hierdurch Missbrauch und Manipulation zu verhindern, verstoßen gegen die Bestimmungen der DS-GVO und müssen daher mit Anordnungen im Sinne des Art. 58 Abs. 2 DS-GVO und mit Sanktionen nach Art. 83 Abs. 5 DS-GVO rechnen.

Im Berichtszeitraum haben mich mehrere Anfragen und Beschwerden erreicht, die sich mit der Rechtmäßigkeit der Verarbeitung biometrischer Daten im Beschäftigungsverhältnis befassen. So wandten sich schon zu Beginn des Jahres zwei Beschäftigte eines kleinen mittelständischen Unternehmens unabhängig voneinander an meine Behörde und berichteten von der Nutzung eines Arbeitszeiterfassungssystems mittels Fingerabdrucks im Betrieb ihres Arbeitgebers. Die Beschwerdeführer fragten bei mir an, ob der Einsatz eines solchen Systems ohne ihre Einwilligung datenschutzrechtlich zulässig sei.

Die Anfragen der Beschwerdeführer habe ich zum Anlass genommen, den Verantwortlichen anzuhören und zur Nutzung des biometrischen Arbeitszeiterfassungssystems in seinem Unternehmen zu befragen. In meinem Anhörungsschreiben informierte ich den Verantwortlichen über meine grundsätzlichen Bedenken bezüglich des Einsatzes biometrischer Zeiterfassungssysteme. Ich forderte ihn auf, mir den Zweck und die Rechtsgrundlage für das Datenverarbeitungsverfahren mitzuteilen.

Auf meine Anhörung teilte der Verantwortliche mit, dass er sich für die Einführung des Systems entschieden habe, nachdem es bei dem früher im Einsatz befindlichen Zeiterfassungssystem wiederholt zu Missbrauch und Manipulation durch einzelne Arbeitnehmer gekommen sei. Um hier Abhilfe zu schaffen – was nicht zuletzt im Interesse der rechtstreuen Arbeitnehmer geboten wäre –, sei ein manipulationssicheres System eingeführt worden. Aufgrund des genannten Einsatzzweckes vertrat der Verantwortliche die Auffassung, dass als Rechtsgrundlage Art. 9 Abs. 2 lit. b DS-GVO zur Anwendung gelange, da der Einsatz des biometrischen Zeiterfassungssystems zur Ausübung von Rechten aus dem Arbeitsrecht erforderlich sei.

Während des Prüfungsverfahrens zeigte sich, dass der Einsatz des biometrischen Zeiterfassungssystems in der beschriebenen Ausgestaltung gegen die DS-GVO verstieß. Ich habe dem Verantwortlichen daher mitgeteilt, dass ich beabsichtige, von meinen Befugnissen nach Art. 58 Abs. 2 DS-GVO Gebrauch zu machen. Konkret habe ich in Betracht gezogen, den Verantwortlichen

anzuweisen, das Verarbeitungsverfahren *biometrische Arbeitszeiterfassung mittels Fingerabdrucks* durch Einholung wirksamer Einwilligungserklärungen der Beschäftigten in Einklang mit der DS-GVO zu bringen, vgl. Art. 58 Abs. 2 lit. d DS-GVO, oder ein Verbot zu verhängen, vgl. Art. 58 Abs. 2 lit. f DS-GVO. Darüber hinaus habe ich dem Verantwortlichen mitgeteilt, dass aufgrund der festgestellten Verstöße gegen die Bestimmungen der DS-GVO Sanktionen nach Art. 58 Abs. 2 lit. i i. V. m. Art. 83 Abs. 4 lit. a, Abs. 5 lit. a DS-GVO zu prüfen sind.

Der Verantwortliche teilte mir daraufhin mit, dass er das Verarbeitungsverfahren *biometrische Arbeitszeiterfassung* eingestellt und durch ein RFID-Zeiterfassungssystem ersetzt hat.

Meiner Entscheidung lagen folgende Fragen und Erwägungen zugrunde:

I. Was sind biometrische Daten im Sinne des Art. 4 Ziffer 14 DS-GVO und handelt es sich hierbei um besondere personenbezogene Daten im Sinne von Art. 9 DS-GVO?

Der Europäische Gesetzgeber hat den Begriff der biometrischen Daten in Art. 4 Ziffer 14 DS-GVO definiert. Biometrische Daten sind hiernach mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten (Verfahren zur Auswertung von Fingerabdrücken). Typische personenbezogene Merkmale im Sinne von Art. 4 Ziffer 14 DS-GVO sind etwa Fingerabdruck, Iris, Netzhaut, Gesicht, Handgeometrie oder auch das Handvenenmuster.

Art. 9 Abs. 1 DS-GVO enthält ein generelles Verarbeitungsverbot für besondere Kategorien personenbezogener Daten. Hierunter fallen nach dem Wortlaut der Vorschrift auch die zuvor beschriebenen biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person.

II. Biometrische Arbeitszeiterfassung mittels Fingerabdruck – wie funktioniert das?

Mit dem Begriff des Fingerabdrucks wird der Abdruck der sog. Papillarleisten am Endglied eines Fingers beschrieben. Diese Papillarleisten lassen sich durch verschiedene Merkmale unterscheiden: Grundmuster, grobe Merkmale, feinere Merkmale wie Gabelung und Linienendung (sog. Minuzien) und Porenstruktur.

Aufgrund der verschiedenen Charakteristika sowie ihrer individuellen Verteilung wird von der Einzigartigkeit des Fingerabdrucks jeder Person ausgegangen.

Soll der Fingerabdruck – etwa zur Arbeitszeiterfassung – genutzt werden, bedeutet dies in der Regel, dass mit Hilfe eines Fingerabdrucklesers zunächst eine Fingerabdruckanalyse ausgeführt wird. Hierbei werden die Minuzien herausgefiltert. Die Minuzien werden mittels spezieller Algorithmen in eine mathematische Form gebracht (Merkmalsvektor 1). Der Merkmalsvektor 1 wird anschließend abgespeichert, z. B. in einer Datenbank oder auf einer Chipkarte. Ein konkreter Fingerabdruck ist aus dem Merkmalsvektor 1 nicht mehr rekonstruierbar. Erfolgt anschließend ein erneutes Einlesen des Fingerabdrucks, errechnet das System anhand der Minuzien einen Merkmalsvektor 2 und einen Vergleichswert (Schwellwert) zwischen Merkmalsvektor 1 und 2. Überschreitet der errechnete Vergleichswert der beiden Merkmalsvektoren einen bestimmten Deckungsgrad, wird die Person erkannt und die Aufzeichnung der Arbeitszeit mittels Fingerabdrucks gestartet bzw. beendet.

Ausführliche Informationen zu diesem Thema enthält das Positionspapier zur biometrischen Analyse der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder vom 03.04.2019, das über die Webseite der DSK unter *https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf* abgerufen werden kann.

III. Warum verstößt die biometrische Arbeitszeiterfassung mittels Fingerabdrucks in dem zugrundeliegenden Fall gegen die Bestimmungen der DS-GVO?

1. *Der Erlaubnisvorbehalt und das Verbotsprinzip der DS-GVO, vgl. Art. 5 Abs. 1 i. V. m. Art. 6 Abs. 1 DS-GVO und Art. 9 Abs. 1 DS-GVO*

Art. 5 Abs. 1 lit. a bis f DS-GVO beschreibt die Grundsätze für die Verarbeitung personenbezogener Daten. Nach Art. 5 Abs. 1 lit. a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Durch die Regelung des Art. 5 Abs. 1 lit. a DS-GVO wird bestimmt, dass die Verarbeitung personenbezogener Daten nur bei Vorliegen eines gesetzlichen Erlaubnistatbestandes zulässig ist (sog. Erlaubnisvorbehalt). Die Vorschrift des Art. 6 Abs. 1 lit. a – f) DS-GVO enthält die Erlaubnistatbestände, die eine Verarbeitung personenbezogener Daten rechtfertigen können.

Für die Verarbeitung besonderer Kategorien personenbezogener Daten, worunter auch biometrische Daten im Sinne des Art. 4 Ziffer 14 DS-GVO fallen,

sind die gesetzlichen Anforderungen noch strenger: Art. 9 Abs. 1 Satz 1 DS-GVO untersagt die Verarbeitung besonderer Kategorien personenbezogener Daten (**Verbotsprinzip**). Eine abschließende Aufzählung der Ausnahmen vom Verarbeitungsverbot enthält Art. 9 Abs. 2 DS-GVO.

Ausgehend von dem beschriebenen Fall folgt hieraus, dass – sofern für das biometrische Zeiterfassungssystem mittels Fingerabdrucks beim Verantwortlichen kein Ausnahmetatbestand des Art. 9 Abs. 2 DS-GVO greift –, die Nutzung des Systems verboten ist, vgl. Art. 9 Abs. 1 DS-GVO.

2. *Warum liegen die Voraussetzungen eines Ausnahmetatbestandes im Sinne von Art. 9 Abs. 2 DS-GVO i. V. m. § 26 Abs. 3 Satz 1 BDSG nicht vor?*

Wie bereits eingangs erwähnt, hat der Verantwortliche im Rahmen des Anhörungsverfahrens vorgetragen, dass er sich für die Einführung des Systems entschieden habe, nachdem es bei dem früher im Einsatz befindlichen Zeiterfassungssystem wiederholt zu Missbrauch und Manipulation durch einzelne Arbeitnehmer gekommen sei. Um hier Abhilfe zu schaffen – was nicht zuletzt im Interesse der rechtstreuen Arbeitnehmer geboten wäre –, sei ein manipulationssicheres System eingeführt worden.

Aufgrund des genannten Einsatzzweckes vertrat der Verantwortliche die Auffassung, dass als Rechtsgrundlage Art. 9 Abs. 2 lit. b DS-GVO zur Anwendung gelange. Die Vorschrift enthält eine Ausnahme vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten u. a. für den Fall, dass die Verarbeitung erforderlich ist, damit der Verantwortliche die ihm aus dem Arbeitsrecht zustehenden Rechte ausüben kann. Durch den in der Vorschrift enthaltenen Zusatz „*soweit dies nach Unionsrecht oder dem Recht der Mitgliedsstaaten (…) zulässig ist*“ macht der Europäische Gesetzgeber deutlich, dass Art. 9 Abs. 2 lit. b DS-GVO eine unionsrechtliche oder mitgliedsstaatliche Regelung verlangt. Die Vorschrift ist für sich genommen somit keine Rechtsgrundlage, welche die Verarbeitung besonderer Kategorien personenbezogener Daten gestattet.

Für den Bereich des Beschäftigtendatenschutzes enthält eine solche Regelung aber § 26 Abs. 3 Satz 1 BDSG. Nach dem Wortlaut der Vorschrift ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO für Zwecke des Beschäftigungsverhältnisses unter anderem dann zulässig, wenn sie zur Ausübung von Rechten aus dem Arbeitsrecht erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt (vgl. auch BT-Drs. 18/11325, 102).

Zentral ist hier zum einen der Begriff der Erforderlichkeit: Nach dem Willen des deutschen Gesetzgebers sind im Rahmen der Erforderlichkeitsprüfung die betroffenen Grundrechtspositionen und widerstreitenden Interessen zur Herstellung praktischer Konkordanz abzuwägen und zu einem Ausgleich zu bringen, der die Interessen des Verantwortlichen und die von der Verarbeitung betroffenen Personen möglichst weitgehend berücksichtigt (BT-Drs. 18/11325, 101). Zu fordern ist hierfür eine Prüfung am Maßstab des Verhältnismäßigkeitsgrundsatzes, was wiederum voraussetzt, dass seitens des Verantwortlichen ein legitimer Zweck verfolgt wird, das Verarbeitungsverfahren für die Verwirklichung dieses Zwecks geeignet ist und es sich um das mildeste aller gleich effektiv zur Verfügung stehenden Mittel handelt (vgl. BAG, Beschluss vom 9.4.2019 – 1 ABR 51/17, 39 = NZA 2019, 1055 (1059)).

Zusätzlich zur Verhältnismäßigkeitsprüfung im Rahmen der Erforderlichkeit darf kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen der betroffenen Beschäftigten die Interessen des Verantwortlichen überwiegen (BT-Drs. 18/11325, 102).

Nur wenn die zuvor beschriebenen Voraussetzungen erfüllt sind, kann die Verarbeitung der Fingerabdruckdaten von Beschäftigten zum Zwecke der Arbeitszeiterfassung auf die Rechtsgrundlage des § 26 Abs. 3 Satz 1 BDSG gestützt werden. Ob eine biometrische Arbeitszeiterfassung daher überhaupt den Anforderungen des § 26 Abs. 3 Satz 1 BDSG genügen kann, ist fraglich.

Soweit die biometrische Arbeitszeiterfassung mittels Fingerabdrucks den Zweck der Verhinderung der Manipulation von Zeiterfassungsdaten erfüllen soll, sind die Voraussetzungen des § 26 Abs. 3 Satz 1 BDSG schon bei einer Gesamtschau mit § 26 Abs. 1 Satz 2 BDSG nicht erfüllt.

Zwar mag die Arbeitszeiterfassung der Ausübung von Rechten aus dem Arbeitsrecht dienen, vgl. § 26 Abs. 3 Satz 1 BDSG i. V. m. § 611 a Abs. 1 Satz 1 und 2 BGB. Soweit der Arbeitgeber die biometrische Arbeitszeiterfassung mittels Fingerabdrucks aber gerade zum Zwecke der Verhinderung der Manipulation von Zeiterfassungsdaten einführt, fördert dies die Annahme des Arbeitgebers zutage, dass die Beschäftigten seines Unternehmens Straftaten begehen, namentlich den Tatbestand des Arbeitszeitbetruges gemäß § 263 StGB erfüllen (so auch LAG Berlin-Brandenburg, Urteil vom 4.6.2020 – 10 Sa 2130/19, 71). Für die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten im Beschäftigungsverhältnis sieht § 26 Abs. 1 Satz 2 BDSG eine spezialgesetzliche Regelung vor. Die Vorschrift gestattet die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten nur bei Vorliegen strenger Voraussetzungen, etwa wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht einer Straftat im

Beschäftigungsverhältnis begründen und die Verarbeitung zur Aufdeckung der Straftat erforderlich ist, vgl. § 26 Abs. 1 Satz 2 BDSG.

Wenn § 26 Abs. 1 Satz 2 BDSG aber für die Verarbeitung personenbezogener Daten u. a. verlangt, dass „*zu dokumentierende tatsächliche Anhaltspunkte*" den Verdacht einer Straftat begründen, warum sollten dann an die Verarbeitung der schutzbedürftigeren besonderen Kategorien personenbezogener Daten geringere Anforderungen zu stellen sein (vgl. insoweit die zutreffenden Ausführungen des LAG Berlin-Brandenburg, Urteil vom 4.6.2020 – 10 Sa 2130/19, 72)? Ein solches Verständnis würde sowohl der gesetzlichen Systematik als auch dem Sinn und Zweck der Vorschrift widersprechen.

Darüber hinaus ist zu beachten, dass ein Grundrechtseingriff von hoher Intensität bereits als solcher unverhältnismäßig sein kann, wenn der Eingriffsanlass kein hinreichendes Gewicht aufweist (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07, 244). Soweit der Eingriff der Abwehr bestimmter Gefahren dient, kommt es für das Gewicht des Eingriffsanlasses maßgeblich auf den Rang und die Art der Gefährdung der Schutzgüter an (wie zuvor). Der mit der biometrischen Zeiterfassung mittels Fingerabdrucks verbundene Eingriff in das Persönlichkeitsrecht ist bereits aufgrund der Wertungen des Art. 9 Abs. 1 DS-GVO von hoher Intensität, so dass das Interesse des Arbeitgebers an einer „manipulationssicheren" Arbeitszeiterfassung mittels Fingerabdrucks demgegenüber zurücktreten muss (so auch LAG Berlin-Brandenburg, Urteil vom 4.6.2020 – 10 Sa 2130/19, 72).

3. *Könnte die Einführung eines biometrischen Zeiterfassungssystems auf Basis wirksamer Einwilligungen der Beschäftigten nach § 26 Abs. 3 Satz 2 BDSG datenschutzkonform möglich sein?*

§ 26 Abs. 3 Satz 2 BDSG ermöglicht dem Verantwortlichen die Verarbeitung besonderer Kategorien personenbezogener Daten – mithin auch biometrischer Daten – auf der Grundlage einer sich ausdrücklich auf diese Daten beziehenden Einwilligung der Beschäftigten. Es ist daher nicht auszuschließen, dass Arbeitgeber ein biometrisches Zeiterfassungssystem auf Basis wirksamer Einwilligungserklärungen der Beschäftigten datenschutzkonform einführen und nutzen können.

Die Anforderungen an eine wirksame Einwilligungserklärung sollten von Verantwortlichen jedoch nicht unterschätzt werden: Neben § 26 Abs. 3 Satz 2 BDSG sind die Voraussetzungen des § 26 Abs. 2 BDSG zu beachten. Darüber hinaus ist der Verantwortliche für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss deren Einhaltung nachweisen können (Rechenschaftspflicht), vgl. Art. 5 Abs.

2 DS-GVO. Verantwortliche sollten sich mit Blick auf den Einwilligungsprozess und die Ausgestaltung der Einwilligungserklärung daher z. B. folgende Fragen stellen:

– Ist die Einwilligung überhaupt für die geplante Datenverarbeitung geeignet?

Dies setzt voraus, dass die Einwilligung jederzeit (mit Wirkung für die Zukunft) widerrufen und der Datenverarbeitungsprozess – je nach Willensbekundung der betroffenen Beschäftigten – „unterschiedlich" ausgestaltet werden kann (Alternativverhalten). Speziell für die biometrische Arbeitszeiterfassung muss daher eine alternative Möglichkeit der Zeiterfassung vorgesehen werden (z. B. mittels Chipkarte oder Token).

– Kann von einer informierten Willensbekundung ausgegangen werden?

Dies setzt voraus, dass dem Beschäftigten verständlich gemacht wird, zu welchem Zweck die Verarbeitung seiner personenbezogenen Daten erfolgt und wie das Verfahren ausgestaltet ist. Mit Blick auf die Rechenschaftspflicht des Verantwortlichen empfiehlt es sich, die Informationen in Textform in einer klaren und einfachen Sprache zur Verfügung zu stellen. Gemäß § 26 Abs. 3 Satz 1 BDSG ist darüber hinaus sicherzustellen, dass sich die Einwilligung der betroffenen Beschäftigten ausdrücklich auf die Verarbeitung biometrischer Daten bezieht.

– Wurden die betroffenen Beschäftigten über ihr Widerrufsrecht aufgeklärt?

Die Informationen über das Widerrufsrecht sind nach § 26 Abs. 2 Satz 3 BDSG in Textform zur Verfügung zu stellen.

– Erfolgt die Einwilligung der Beschäftigten auf freiwilliger Basis?

§ 26 Abs. 2 Satz 1 und 2 BDSG messen der Frage der Freiwilligkeit der Einwilligung im Beschäftigungskontext besondere Bedeutung zu. Dies trägt dem Umstand Rechnung, dass zwischen Arbeitgeber und Beschäftigten ein Über-/Unterordnungsverhältnis besteht. Die Einwilligung kommt für Verarbeitungen von Beschäftigtendaten daher regelmäßig nicht in Betracht (vgl. auch Kurzpapier Nr. 14 Beschäftigtendatenschutz der DSK). Insbesondere wenn es um die Frage der Freiwilligkeit der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten geht, ist nach dem Willen des Gesetzgebers ein strenger Maßstab anzulegen (vgl. auch BT-Drs. 18/11325, 102). Verantwortliche sollten sich daher fragen, ob sich die Problematik des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer in Hinblick auf die geplante Datenverarbeitungssituation auswirkt,

unter welchen tatsächlichen Umständen/ Gegebenheiten die Einwilligung bei den Betroffenen eingeholt wird (Möglichkeit des Entstehens von Druck-Situationen) und ob die Einwilligung in unzulässiger Weise an weitergehende Bedingungen „gekoppelt“ ist. Als Fallkonstellationen, bei deren Vorliegen von der Freiwilligkeit der Einwilligung ausgegangen werden kann, nennt § 26 Abs. 2 Satz 3 BDSG das Bestehen eines rechtlichen oder wirtschaftlichen Vorteils des Beschäftigten sowie das Verfolgen gleichgelagerter Interessen von Arbeitgebern und Beschäftigten.

– Werden die Formerfordernisse für die Einwilligung im Beschäftigungsverhältnis beachtet?

Nach § 26 Abs. 2 Satz 3 BDSG hat die Einwilligung schriftlich oder elektronisch zu erfolgen, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist.

– Kann der Verantwortliche nachweisen, dass die betroffene Person wirksam in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat?

Hierüber sollten sich Verantwortliche insbesondere vor dem Hintergrund der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht Gedanken machen.

7.2
Kostenprüfung bei Gesundheitsleistungen für Asylbewerber

Es besteht ein berechtigtes Interesse der öffentlichen Hand, die korrekte Rechnungsstellung seitens der Erbringer von Gesundheitsleistungen (insbesondere Kliniken, Ärzte) für Asylbewerber zu überprüfen. Die Asylbewerber sind verpflichtet, die wegen der ärztlichen Schweigepflicht erforderliche Einwilligung in die für die Abrechnungsüberprüfung notwendige Datenverarbeitung zu erteilen.

Das Hessische Ministerium für Soziales und Integration unterbreitete mir einen das Asylbewerberleistungsrecht betreffenden Sachverhalt und bat um datenschutzrechtliche Beratung. Konkret ging es darum, dass nach dem Asylbewerberleistungsgesetz (§§ 4 und 6 AsylbLG) Asylsuchende Anspruch auf notwendige ärztliche Versorgung haben.

In den Erstaufnahmeeinrichtungen in Hessen wird in eigenen medizinischen Ambulanzen die ärztliche Grundversorgung gewährleistet. Für eine darüber hinausgehende Diagnostik und Therapie werden die Asylbewerber an externe Fachärzte / -kliniken überwiesen. Diese externen medizinischen Leistungserbringer adressieren anschließend die kostenmäßige Abrechnung an

das Regierungspräsidium Gießen. Das RP Gießen hat dann die Richtigkeit der Abrechnung zu überprüfen. Dieser Ablauf findet ohne Beteiligung von Krankenkassen statt.

Medizinische Versorgung bei Krankenversicherten (Sozialgesetzbuch V)

Gesetzliche Krankenkassen sind verpflichtet, zur Prüfung der ordnungsgemäßen Abrechnung seitens der Leistungserbringer eine gutachterliche Stellungnahme des Medizinischen Dienstes (MDK) einzuholen. Haben Krankenkassen bzw. der MDK für eine gutachterliche Stellungnahme oder Prüfung erforderliche Daten der versicherten Person bei den Leistungserbringern angefordert, so sind die Leistungserbringer gesetzlich verpflichtet, diese Daten an den MDK zu übermitteln. Soweit im Einzelfall eine gutachterliche Stellungnahme betreffend die Notwendigkeit und Dauer einer stationären Behandlung erforderlich ist, ist das ärztliche Personal des MDK befugt, Räume von Krankenhäusern und Vorsorge- oder Rehabilitationseinrichtungen zu betreten. Der Ablauf ist im Sozialgesetzbuch V – Gesetzliche Krankenversicherung – näher geregelt (§ 275 Abs. 1, § 276 Abs. 2 und 4 SGB V).

Unterschied zwischen Sozialgesetzbuch V (Krankenversicherung) und Asylbewerberleistungsrecht

Dieses im Sozialgesetzbuch V normierte Prüfverfahren ist im Asylbewerberleistungsgesetz allerdings nicht vorgesehen. Die Möglichkeit einer zumindest stichprobenartigen Krankenhausrechnungsüberprüfung oder einer Plausibilitätskontrolle der Behandlungsabrechnungen gestalte sich, so berichtete mir das Ministerium, nach Angaben des RP Gießen aus Gründen der ärztlichen Schweigepflicht schwierig. Das RP Gießen habe das Problem näher beschrieben, dass sich rechnungsstellende Krankenhäuser darauf berufen, Arztbriefe oder Dokumentationen wegen der ärztlichen Schweigepflicht nicht herausgeben zu dürfen. Hierdurch, so das Ministerium, entstehe eine Diskrepanz zwischen Zahlungspflicht der öffentlichen Hand einerseits und nicht möglicher korrekter Rechnungsüberprüfung andererseits.

Vor diesem Hintergrund sei es geboten, so das Ministerium, dass dem MDK im Asylbewerberbereich ein umfassendes Prüfrecht mit Blick auf die von Leistungserbringern geltend gemachten Kosten eingeräumt werde.

Datenschutzaufsichtsbehördliche Bewertung und Beratung

Im Bereich der gesetzlichen Krankenversicherung, SGB V, gibt es hinreichend gesetzlich verankerte Prüfbefugnisse für die Krankenkassen bzw. den MDK und eine dementsprechende Auskunftspflicht der Leistungserbringer.

Bei Leistungen nach dem Asylbewerberleistungsgesetz handelt es sich nicht um Leistungen nach dem Sozialgesetzbuch V. Insoweit können die Regelungen dieses Gesetzbuchs, die die Rechnungsprüfung betreffen, nicht im Asylbewerberbereich angewendet werden. Vergleichbare Regelungen zu Prüfrechten oder Auskunftspflichten zwischen Kostenträgern und Leistungserbringern kennt das Asylbewerberleistungsrecht allerdings nicht.

In einigen Bundesländern werden jedoch die Leistungen nach § 4 AsylbLG von gesetzlichen Krankenkassen übernommen („Bremer Modell“). Der Gesetzgeber hat dieses Konzept in der umfangreichen Vorschrift § 264 SGB V generell geregelt. Im Rahmen dieser Lösung können dann die Krankenkassen bzw. der MDK hinsichtlich der Rechnungsüberprüfung entsprechend §§ 275 f. SGB V vorgehen.

Hessen hat bislang die Erbringung der Leistungen jedoch nicht über die Krankenkassen abgewickelt, sodass hinsichtlich der Prüf- und Auskunftsvorschriften auch nicht auf das Sozialgesetzbuch V rekurriert werden kann.

Insoweit stehen die DS-GVO und speziell die ärztliche Schweigepflicht einer Prüfberechtigung des Kostenträgers und einer Auskunft der Leistungserbringer entgegen.

Kein Verstoß gegen die ärztliche Schweigepflicht im Fall der Einwilligung

Die ärztliche Schweigepflicht wird im Fall einer Kostenüberprüfung allerdings nicht verletzt, wenn eine Einwilligung desjenigen vorliegt, um dessen personenbezogene Daten es geht. Denn in diesem Fall ist die Datenverarbeitung nach der Europäischen Datenschutzgrundverordnung zulässig, Art. 6 Abs. 1 a) DS-GVO.

Art. 6 DS-GVO

(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.

Da es im vorliegenden Kontext freilich auch um sensible Daten der Asylbewerber geht, nämlich insbesondere Ethnie und Gesundheitsdaten der Asylbewerber, ist zusätzlich Art. 9 DS-GVO zu beachten, der personenbezogene Daten sensibler Art betrifft. Aber auch diese Vorschrift eröffnet im Fall der Einwilligung den Weg zur rechtmäßigen Datenverarbeitung, Art. 9 Abs. 1, Abs. 2 a) DS-GVO.

Art. 9 DS-GVO

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft (…) hervorgehen, sowie die Verarbeitung (…) von Gesundheitsdaten einer natürlichen Person ist untersagt.

(2) Abs. 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden.

(…)

Der am Ende des zitierten Normtextes von Art. 9 Abs. 2 a) DS-GVO angesprochene Ausschluss der Einwilligung als Erlaubnistatbestand ist zwar von den deutschen Datenschutzaufsichtsbehörden diskutiert, aber vom Gesetzgeber jedenfalls nicht wahrgenommen worden, so dass auch bei sensiblen Daten die Einwilligung als Rechtfertigung der Datenverarbeitung zur Verfügung steht. Freilich wird gerade im öffentlichen Bereich die DS-GVO noch durch nationales Recht der Mitgliedstaaten ergänzt und komplettiert (Art. 6 Abs. 2 und 3 DS-GVO), das bei der datenschutzrechtlichen Beurteilung zusätzlich zur DS-GVO herangezogen und beachtet werden muss.

Mit Blick auf die vom Hessischen Ministerium für Soziales und Integration mir unterbreitete Thematik der Rechnungsstellung seitens der Erbringer von Gesundheitsleistungen einerseits und der Überprüfungsnotwendigkeit des öffentlichen Kostenträgers andererseits sowie dem Problem der ärztlichen Schweigepflicht enthält nun das Asylbewerberleistungsrecht eine entscheidende Vorschrift, § 9 Abs. 3 AsylbLG, weil diese Regelung nämlich die Mitwirkungsobliegenheiten der Leistungsempfänger im Sozialbereich und eben auch die Obliegenheit der Leistungsempfänger zur Erteilung der erforderlichen Zustimmungen (Einwilligungen) für die Aufgabenwahrnehmung der öffentlichen Leistungsverwaltung in Bezug nimmt und entsprechend für anwendbar erklärt, nämlich § 9 Abs. 3 AsylbLG.

§ 9 AsylbLG

(…)

(3) Die §§ 60 bis 67 des Ersten Buches des Sozialgesetzbuchs über die Mitwirkung des Leistungsberechtigten sind entsprechend anzuwenden.

Die Vorschrift hat ihren Hintergrund gerade darin, dass das Asylbewerberleistungsrecht rechtssystematisch zwar nicht dem Sozialrecht gesetzlich zugeordnet worden ist (vgl. § 68 SGB I), es aber gleichwohl geboten ist, die für die Leistungsempfänger im Sozialrecht normierten Mitwirkungspflichten auch den Empfängern von Asylbewerberleistungen aufzuerlegen. Das bedeutet konkret, dass diejenigen, die ärztliche/medizinische Leistungen in Anspruch nehmen, sich damit einverstanden zu erklären haben, dass die Richtigkeit/Angemessenheit der für diese Leistungen von den Kliniken, Ärzten etc. eingereichten Rechnungen von der öffentlichen Verwaltung als Leistungs- und Kostenträger auch effektiv kontrolliert werden kann. Deshalb ordnet das Sozialrecht an, dass insbesondere wegen der ärztlichen Schweigepflicht notwendige Einwilligungen mit Blick auf die erforderliche Aufgabenwahrnehmung der öffentlichen Verwaltung (hier Rechnungsprüfung) vom Leistungsempfänger zu erteilen sind, § 60 Abs. 1 Nr. 1 SGB X.

§ 60 SGB I

(1) Wer Sozialleistungen beantragt oder erhält, hat

1. alle Tatsachen anzugeben, die für die Leistung erheblich sind, und auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen.

(…)

Die entsprechende Anwendung dieser Vorschrift im Asylbewerberbereich bedeutet deshalb vor allem, dass die zuständige Asylbewerberleistungsbehörde von den betroffenen Asylbewerbern die Zustimmung hinsichtlich der erforderlichen Auskünfte seitens der Leistungserbringer (Klinik, Ärzte) einfordern kann.

Das anfragende Ministerium für Soziales und Integration habe ich auf diese Rechtslage hingewiesen.

7.3
Es bleibt dabei: Keine umfassenden Bildaufnahmen in der Kita ohne Beachtung datenschutzrechtlicher Anforderungen

Die Anfertigung von Foto- (und Video-) Aufnahmen in Kindertagesstätten bzw. Kindergärten bleibt ein sensibles datenschutzrechtliches Dauerthema. Die verantwortlichen Stellen sind seit Inkrafttreten der DS-GVO nochmals mehr in der Pflicht, umfassende technische und organisatorische Maßnahmen zu treffen und für die nötige Transparenz gegenüber den Eltern/Sorgeberechtigten zu sorgen, – für alle damit in Zusammenhang stehenden Vorgänge (von der Fertigung bis zur weiteren Verwendung) und zum weiteren Umgang dieser Aufnahmen.

Mich erreichte eine Beschwerde eines betroffenen Elternteils über eine Kindertagesstätte bzw. den (freien) Träger dieser Kindertagesstätte, in der bzw. bei dem eines der Kinder des Beschwerdeführers aufgenommen werden sollte. Der Träger betreibt im Übrigen auch noch andere Kindertagesstätten an anderen Orten.

Gegenstand der Beschwerde waren den Datenschutz adressierende Passagen, in dem vom Träger dort in der Kindertagesstätte eingesetzten (umfangreichen) Vertrag zur Kinderbetreuung. Dieser Vertrag enthielt z. B. an einer Stelle auch einen Passus zum „Erstellen und Verbreiten von Foto- und Filmaufnahmen“. Die Datenschutzregelungen im gesamten Vertrag erschienen dem Beschwerdeführer nicht haltbar zu sein und gegen geltendes Datenschutzrecht zu verstoßen. Die Möglichkeit, einzelnen Passagen und deren Regelungen zu widersprechen, sah der Träger nicht vor. Eine Betreuungsmöglichkeit wurde nur durch vollständige Vertragsunterzeichnung der Eltern/Sorgeberechtigten eröffnet.

Darum involvierte der Betroffene mich, bat um meine Prüfung und Intervention.

Einleitung

Das Thema Foto- und Filmaufnahmen in Kindertagesstätten bzw. Kindergärten ist seit vielen Jahren ein Dauerthema im Bereich Sozialwesen und regelmäßig/alljährlich Gegenstand von Beschwerden, Beratungsanfragen, Prüfanträgen usw.

Die Sensibilität dieses Themas liegt auf der Hand, denn die besondere Schutzbedürftigkeit von Kindern ist unmittelbar eingängig wie offenkundig und schlägt sich nicht zuletzt z. B. in der grundgesetzlich niedergelegten (sog.) Wächteraufgabe des Staates nieder.

Die – teils – seit Jahren oder gar Jahrzehnten geltenden Gesetze und Aufgaben des Staates im Zusammenhang mit dem Schutz von Kindern und Jugendlichen sind seit Inkrafttreten der DS-GVO aus datenschutzrechtlicher Perspektive nochmals ausdrücklich und zusätzlich geschärft worden, indem die DS-GVO die besondere Schutzbedürftigkeit von Kindern und Jugendlichen an mehreren Stellen ausdrücklich erwähnt (vgl. nur z. B. Art. 6 Abs. 1 lit. f, Art. 8 oder Erw.Gr. 38 DS-GVO).

Insofern ist und bleibt es auch für mich ein gewichtiges Thema, das im Rahmen von Beschwerden und Anfragen aufmerksam und kritisch begleitet und, sofern erforderlich, auch mit Nachdruck gegenüber verantwortlichen Stellen für datenschutzaufsichtsbehördlich akzeptable Lösungen verfolgt wird.

Sachverhalt und rechtliche Bewertung

Der Beschwerdeführer reichte mir neben seiner Beschwerde auch den vollständigen, von ihm kritisierten Betreuungsvertrag des Trägers ein. Nach dessen kritischer Durchsicht musste ich einerseits zu unbestimmte und intransparente Regelungen unter einer Regelung zum Datenschutz konstatieren. Andererseits stachen tatsächlich die dortigen Ausführungen und Regelungen zum „Erstellen und Verbreiten von Foto- und Filmaufnahmen“ ins Auge, so z. B. insbesondere folgender Passus:

„Die Erziehungsberechtigten willigen mit ihrer Unterschrift dieses Vertrages in das Verbreiten bzw. öffentliche zur Schau stellen von Aufnahmen, auf denen auch ihr Kind bzw. sie selbst zu sehen sind, für folgende Zwecke – auch nach Beendigung des Betreuungsverhältnisses – unter dem Vorbehalt ein, dass keine schutzwürdigen Interessen des Kindes und der Familie beeinträchtigt werden.

– *Verwenden von Foto-, Dia-Aufnahmen, die das Personal erstellt, für Druck-Erzeugnisse (z. B. Einrichtungskonzept, Elternbriefe, Jahresberichte, Chroniken, Foto-Galerie im geschützten Elternbereich).*
– *Vorführen von Foto-, Film-, Dia-Aufnahmen, die das Personal oder eine andere Person im Auftrag erstellt, auf Elternabenden, in kommunalpolitischen Gremien und anderen Kreisen einer interessierten Öffentlichkeit.*
– *Veröffentlichen von Foto- und Film-Aufnahmen, die das Personal oder ein Pressevertreter erstellt, in Presseberichten über die Einrichtung.“*

Ohne zu sehr ins Detail zu gehen, waren weite Teile der Regelungen zum Datenschutz und zum Umgang mit Foto- und Filmaufnahmen zu oder völlig unbestimmt („Pauschalaussagen“), so dass z. B. eine wirksame Einwilligung

der Eltern/Sorgeberechtigten schon gar nicht erteilt werden konnte, weil diese das Ausmaß der Datenverarbeitung beim Träger nicht erkennen und einschätzen konnten. Sie wurden schlicht nicht in die Lage versetzt, erkennen zu können, wozu genau sie ihre Einwilligung erteilen sollen.

Auch die im Vertrag erwähnte „uneingeschränkte" Möglichkeit der Verwendung von personenbezogenen Daten für interne Zwecke oder gar untereinander zwischen den verschiedenen Tochtergesellschaften (Kindertagesstätten) musste als inakzeptabel thematisiert werden.

Schließlich und nicht zuletzt galt dies auch für den oben zitierten Passus, der als datenschutzrechtlich inakzeptabel gelten muss.

Ich habe den Träger der Kindertagesstätte(n) daher mit meinen Bedenken konfrontiert. In einer kurzfristigen ersten Reaktion auf mein diesbezügliches Schreiben durch die Rechtsbeiständin des Verantwortlichen hat sich dann – durchaus glücklicherweise – eine meine Bedenken und deutlichen Hinweise dankend aufnehmende, konstruktive Aufarbeitung des Vertrags insgesamt und des Themas „Erstellen und Verbreiten von Foto- und Filmaufnahmen" als Schwerpunkt ergeben.

Die ausgeprägte Kooperationsbereitschaft, gerade in Form der Entgegen- und Aufnahme meiner Kritikpunkte mit sofortiger Anpassung und Umsetzung in das dortige Vertragswerk, stellte sich schnell als positiv bemerkenswert wie inhaltlich verlässlich heraus.

So wurde – es folgt eine beispielhafte Kurzaufzählung – eine den Erfordernissen der DS-GVO (vgl. Art. 12 und 13 DS-GVO) gerecht werdende Datenschutzinformation neu formuliert und integriert. Ferner wurde eine – wegen des Kopplungsverbots gemäß Art. 7 Abs. 4 DS-GVO – vom Vertrag über die Betreuungsleistungen unabhängige Einwilligungserklärung für die Fertigung und Verwendung von (stehenden und laufenden) Aufnahmen von Personen entworfen, die den Anforderungen der Art. 6 Abs. 1 S. 1 lit. a, Art. 7 DS-GVO sowie des § 22 KUG genügt. Hier wurden u. a. auch bestimmte Situationen, in denen überhaupt Aufnahmen in Betracht kommen bzw. gemacht werden, ausgewählt und genau definiert.

Ebenfalls wurde – auch im Zusammenhang der Foto- und Videoaufnahmen – das IT-Sicherheitskonzept nochmals kritisch geprüft, überarbeitet und neu implementiert.

Im Ergebnis wurden durch die wechselseitige und durchweg konstruktive Zusammenarbeit zwischen dem Träger und mir innerhalb kurzer Zeit sowohl das Vertragswerk als auch die technischen und organisatorischen Maßnahmen datenschutzkonform überarbeitet und schnell in die Praxis umgesetzt,

so dass ich von meinen Befugnissen nach Art. 58 DS-GVO keinen Gebrauch machen musste.

Fazit

Vertragsregelungen oder Einwilligungserklärungen in Kindertagesstätten bzw. Kindergärten sind aus datenschutzaufsichtsbehördlicher Perspektive nicht selten problematisch oder gar – in manchen Fällen – inakzeptabel, weil sie die datenschutzrechtlichen Anforderungen nicht erfüllen. Da es hierfür aus verschiedenen Gründen kein einheitliches Muster gibt und geben kann, wird dieses Thema mich auch weiterhin beschäftigen. Dies kann allerdings auch einmal Freude bereiten, wenn ich mich mit einem zugänglichen, kooperativen und verlässlichen Gegenüber auseinandersetzen darf, dem meine Forderungen nachvollziehbar sind und der diese dankend und verlässlich wie umgehend umsetzt.

8. Gesundheitswesen

8.1
Fiebermessen als Zutrittsvoraussetzung für Besucher und Patienten in Krankenhäusern

Aufgrund der Corona-Pandemie hatte ich mich im Berichtszeitraum mit speziellen datenschutzrechtlichen Fragestellungen im Bereich Gesundheit zu beschäftigen. So verhielt es sich auch bei dem nachfolgend geschilderten Vorgang: Ein Krankenhaus beabsichtigte, bei Patienten und Besuchern vor Zutritt des Krankenhauses Fieber zu messen, um frühzeitig Covid-19 Verdachtsfälle zu erkennen.

Die Anfrage beschäftigte sich mit der datenschutzrechtlichen Zulässigkeit von Fiebermessen als Zutrittsvoraussetzung für Besucher und Patienten von Krankenhäusern während der COVID-19 Pandemie. Das Fiebermessen erfolgte bei Liegend-Einweisungen händisch, in allen übrigen Fällen automatisiert mittels installierter Wärmebildkamera im Eingangsbereich des Krankenhauses. Auf die Videoaufnahme und das Fiebermessen wurde dabei mit Informationstafeln hingewiesen. Die Ergebnisse der automatisierten Messung wurden auf einem Monitor am Infopoint in einem separierten Bereich angezeigt, zu dem nur berechtigte Personen Zutritt hatten. Das System meldete betroffene Personen, bei denen eine Körpertemperatur von über 39°C festgestellt worden war.

Getroffene Maßnahmen

Im Dialog mit mir wurden folgende Maßnahmen getroffen: Die automatisiert erhobenen Messdaten und Videoaufnahmen wurden lediglich auf dem Hauptspeicher des Rechners abgelegt. Eine Speicherung auf einer Festplatte erfolgte nicht. Dies hatte zur Folge, dass die Daten nur für kurze Zeit abrufbar sind und mit Herunterfahren des Computers unwiederbringlich gelöscht werden. Außerdem erfolgte keine Verbindung des Computers, der die Messdaten automatisiert erhob, mit dem Kliniknetzwerk (Stand-Alone-System).

Auch konnten die Daten technisch nur abgerufen werden, sofern der voreingestellte Temperaturwert von 39°C überschritten wurde. Von der technischen Seite konnte damit das Zugriffsrisiko durch unberechtigte Personen erheblich reduziert werden. Rechtlich erhielt nur eine begrenzte Anzahl von Mitarbeiterinnen und Mitarbeitern Zugang zu den Räumlichkeiten und Zugriff auf die erhobenen Daten. Die betreffenden Personen wurden zur Verschwiegenheit und Geheimhaltung verpflichtet. Betroffene Personen mit erhöhten Werten

wurden gezielt und diskret durch Pflegepersonal angesprochen und in separaten Räumlichkeiten weiterversorgt.

Rechtliche Bewertung

1. *Anwendungsbereich der DS-GVO und rechtliche Grundlagen*

Nach meiner Auffassung fällt das händische Fiebermessen bei Besuchern oder Patienten grundsätzlich nicht in den Anwendungsbereich der DS-GVO, sofern die Messergebnisse nicht im Gerät gespeichert werden und auch nicht nachträglich in einem Dateisystem abgelegt werden. Es handelt sich hierbei um eine nicht automatisierte Verarbeitung personenbezogener Daten. Der Anwendungsbereich der DS-GVO ist daher nicht eröffnet (Art. 2 Abs. 1 DS-GVO). Anders zu beurteilen ist das händische Fiebermessen bei Mitarbeiterinnen und Mitarbeitern. Hier ist der Anwendungsbereich der DS-GVO auch eröffnet, wenn keine automatisierte Datenverarbeitung erfolgt (siehe u. a. § 26 Abs. 7 BDSG). Auf die Zulässigkeit von Fiebermessen bei Beschäftigten wird an dieser Stelle nicht weiter eingegangen.

Das automatisierte Fiebermessen bei Besuchern, etwa durch Wärmebildkameras, oder eine Verschriftlichung von nicht automatisiert erhobenen Ergebnissen fällt dagegen in den Anwendungsbereich der DS-GVO. Bei den durch die Wärmebildkamera oder händisch erfassten Daten handelt es sich um Gesundheitsdaten, d. h. besondere Kategorien personenbezogener Daten im Sinne des Art. 4 Nr. 1, 9 Abs. 1 DS-GVO. In dem konkret vorliegenden Fall kommt als Rechtsgrundlage der Verarbeitung besonderer Kategorien personenbezogener Daten (hier: Gesundheitsdaten) Art. 6 Abs. 1 lit. e, f, 9 Abs. 1, 2 lit. i DS-GVO in Verbindung mit § 20 Abs. 1 Nr. 3 HDSIG bzw. § 22 Abs. 1 Nr. 1 lit. c BDSG in Betracht.

Zu beachten sind die Voraussetzungen des § 20 Abs. 1 Nr. 3 HDSIG bzw. des § 22 Abs. 1 Nr. 1 lit. c BDSG. So müssen die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person überwiegen. Die Verarbeitung muss in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen und den Wesensgehalt des Rechts auf Datenschutz wahren.

Angesichts der Unberechenbarkeit der Pandemieentwicklung im Jahr 2020 war aus meiner Sicht ein angemessenes Verhältnis von der hier vorgesehenen Datenerhebung zu der Gefährdung von Patienten, Besuchern und Pflegepersonal durch eine Ansteckung zumindest nicht zu verneinen. Allerdings musste die Verhältnismäßigkeit der Datenerhebung stets im Blick behalten werden und im Hinblick auf die Entwicklung der Pandemie immer wieder aufs Neue bewertet werden.

Des Weiteren normiert § 20 Abs. 2 HDSIG bzw. § 22 Abs. 2 BDSG die Pflicht des Verantwortlichen, im Falle der Anwendung einer Rechtsgrundlage aus Abs. 1 spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Die Vorschriften stellen jeweils auf die Implementierung technischer und organisatorischer Maßnahmen ab, die in Bezug auf die konkrete Verarbeitung einen höheren Datenschutz gewährleisten. In diesem Kontext wird auch auf die Parameter Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Faktoren Eintrittswahrscheinlichkeit und Schwere Bezug genommen. Beispielhaft werden Protokollierungen (Nr. 2), Sensibilisierung der Datenverarbeitenden Beteiligten (Nr. 3), aber auch Zugangsbeschränkungen (Nr. 4) genannt. Der Verantwortliche hat demnach unter Berücksichtigung der Umstände des Einzelfalls entsprechende geeignete und angemessene Maßnahmen zu treffen. So muss u. a. sichergestellt werden, dass kein unberechtigter, außenstehender Dritter von den Daten Kenntnis erlangt und die Daten datenschutzkonform vernichtet werden.

2. *Beschluss der Datenschutzkonferenz vom 10.09.2020*

Auch außerhalb des Gesundheitsbereichs wurde im Jahr 2020 die Notwendigkeit des Fiebermessens und dessen Zweckdienlichkeit diskutiert. Teils wurde vorgebracht, dass eine erhöhte Körpertemperatur nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion anzusehen sei. Zudem hätten viele Infizierte keine Symptome und damit auch keine erhöhte Temperatur. Vielmehr stünden mildere Maßnahmen wie zum Beispiel die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der betroffenen Personen zur Verfügung. Aufgrund der genannten Argumente wird auch die Zulässigkeit des Fiebermessens, beispielsweise bei Beschäftigten und Kunden von Industrieunternehmen, durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder abgelehnt (s. a. Anhang I 2.3, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie vom 10.09.2020, abrufbar über die Homepage der DSK).

Der genannte Beschluss der Datenschutzkonferenz gilt allerdings ausdrücklich *nicht* für den Bereich der Gesundheitsversorgung, einschließlich der Pflege. Anders als beispielsweise bei Industrieunternehmen kommt im Bereich der Gesundheitsfürsorge durch Krankenhäuser bei einer Interessenabwägung dem Gesundheitsschutz von Ärzten, Pflegepersonal und Patienten vor einer Infektion mit dem COVID-19 Virus ein größeres Gewicht zu. Die Gesundheit der genannten Personengruppen ist insbesondere in einem Krankenhaus ein besonders empfindliches Gut. Eine qualitativ hochwertige und sichere

Patientenversorgung ist Teil der öffentlichen Daseinsfürsorge und gerade im Falle der Pandemie von besonderer Bedeutung. Die Sicherstellung ausreichenden Klinikpersonals ist hierbei unerlässlich, so dass auch weiterreichende Verarbeitungen von sensiblen Gesundheitsdaten erforderlich und angemessen sein können.

Fazit

Unter der Bedingung besonders strenger technischer Sicherheitsvorgaben und einer umfassenden Informierung der betroffenen Personen, wie sie oben beschrieben wurden, habe ich während der Corona-Pandemie ausnahmsweise das automatisierte Fiebermessen in systemrelevanten Gesundheitseinrichtungen in Einzelfällen für zulässig erklärt, um eine hinreichende gesundheitliche Versorgung der Bürger und einen entsprechenden Schutz des Pflegepersonals sicherzustellen.

8.2
Nutzung eines E-Mail-Verteilers zur Suche nach Patientenakten

Mitarbeiterinnen und Mitarbeiter haben geeignete technische und organisatorische Maßnahmen zu treffen, um unbefugten Personen den Zugriff auf personenbezogene Daten zu verwehren. Dies gilt im besonderen Maße für Gesundheitsdaten. Im vorliegenden Fall wurde ein großer interner E-Mail-Verteiler genutzt, um nicht auffindbare Patientenakten zu suchen.

In einem hessischen Klinikum wurden personenbezogene Daten von Patienten wiederholt und ungefiltert über einen großen internen E-Mail-Verteiler mit über 600 Empfängern versandt. In den meisten Fällen, in denen Patientendaten betroffen waren, ging es insoweit um die Abklärung des Verbleibs einer Patientenakte. Hierzu wurden folgende Patientendaten über den Verteiler versendet:

– Vor- und Nachname,
– Geburtsdatum,
– Dauer des Aufenthalts im Krankenhaus sowie
– die Patienten-Fallnummer der betroffenen Person.

Dieser Verstoß gegen Datenschutzvorgaben, insbesondere gegen Art. 5 Abs. 1 lit. f DS-GVO, wurde dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit mittels einer Eingabe gemeldet.

Getroffene Maßnahmen

Eine bereits bestehende interne Anweisung zum Datenschutz wurde nach Anleitung durch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit an mehreren Stellen überarbeitet. Unter anderem wurde festgeschrieben, dass die Versendung personenbezogener Daten über den E-Mail-Verteiler unzulässig ist. Als Sofortmaßnahme wurde vor Fertigstellung der neuen Datenschutzvorgaben zur Verhinderung weiterer Verstöße eine Rundmail an alle Mitarbeiterinnen und Mitarbeiter versandt.

Darüber hinaus wurde eine Dienstanweisung zur Vorgehensweise bei unklarem Verbleib von Patientenakten erlassen, so dass nunmehr folgende Vorgehensweise festgelegt ist:

1. Patientenakten, deren Verbleib unklar ist, werden zunächst von der Mitarbeiterin oder dem Mitarbeiter individuell über das Krankenhausarchiv angefragt.
2. Sollte die Akte dort nicht aufzufinden sein, werden die Mitarbeiterinnen und Mitarbeiter des Archivs tätig und sprechen die zuletzt involvierten Chefarztsekretariate an.
3. Kann auch hier die Patientenakte nicht aufgefunden werden, darf die Suche maßvoll ausgeweitet werden, jedoch nur über die individuelle Kontaktierung der jeweils zuständigen Mitarbeiterinnen und Mitarbeiter. Eine Nutzung eines E-Mail-Verteilers ist unzulässig.

In Zweifelsfällen ist rechtzeitig der Datenschutzbeauftragte des Klinikums zu kontaktieren.

Darüber hinaus wurde die Nutzung des großen internen E-Mail-Verteilers eingeschränkt. Themen, die von allgemeinem Interesse sind, können nur noch über die Betriebsleitung den jeweiligen Adressaten zur Verfügung gestellt werden. Dies stellt sicher, dass keine persönlichen Daten und erst recht keine sensiblen Gesundheitsdaten unberechtigten Personen zugesandt werden.

Fazit

Bei der Nutzung von internen E-Mail-Verteilern in öffentlichen oder privaten Betrieben ist Vorsicht bei der Versendung persönlicher Daten geboten. Nach Art. 5 Abs. 1 lit. c DS-GVO müssen die verantwortlichen Stellen sicherstellen, dass personenbezogene Daten, wie etwa Namen von Patienten, Geburtsdatum oder die Dauer des Aufenthalts in einem Krankenhaus, vertraulich behandelt werden und vor unbefugtem Zugriff geschützt werden. Auch gilt für die Verarbeitung personenbezogener Daten, wozu auch die Versendung von Patientendaten über einen E-Mail-Verteiler zählt, der Grundsatz der Datenminimierung des Art. 5 Abs. 1 lit. c DS-GVO. Dies hat zur Folge,

dass beispielsweise die Preisgabe personenbezogener Daten nur zulässig ist, wenn dies zur Zweckerreichung erforderlich und angemessen ist. Der vorliegende Fall zeigt, dass ein abgestuftes Modell mit der schrittweisen Erweiterung der Adressaten von persönlichen Daten ausreichend ist. Es ist dahingegen nicht erforderlich, dass von vornherein ein großer Personenkreis Zugriff auf die Daten erhält.

8.3
Datenschutz in Zusammenhang mit der Maskenpflicht im Einzelhandel

Im letzten Jahr erhielt ich eine Vielzahl von Anfragen im Zusammenhang mit der Umsetzung der seit Mai 2020 geltenden Mund-Nasen-Bedeckungspflicht in Geschäften. Der folgende Beitrag gibt Auskunft darüber, wie ich die Bürger in diesem Bereich beraten habe.

Bei der Verpflichtung zum Tragen einer Mund-Nasen-Bedeckung (Maskenpflicht) handelt es sich um eine Schutzmaßnahme gemäß § 28 a Abs. 1 Nr. 2 Infektionsschutzgesetz (IfSG), mit der die Verbreitung der Coronavirus-Krankheit-2019 (COVID-19) verhindert werden soll.

Gemäß § 1 a der Verordnung zur Beschränkung von sozialen Kontakten und des Betriebes von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie (Corona-Kontakt- und Betriebsbeschränkungsverordnung, kurz CoKoBeV) vom 26. November 2020 gilt in vielen Bereichen die Pflicht, eine Mund-Nasen-Bedeckung zu tragen.

Die Ausnahmen von dieser Pflicht findet man in § 1a Abs. 3 CoKoBeV. Danach sind Personen, die aufgrund einer gesundheitlichen Beeinträchtigung oder Behinderung keine Mund-Nasen-Bedeckung tragen können, von der Pflicht, eine Mund-Nasenbedeckung zu tragen, befreit.

Weitere Informationen, wie dies konkret nachzuweisen ist, können der Verordnung leider nicht entnommen werden. Dies führt in der Praxis zu einer großen Verunsicherung, wie damit umgegangen werden soll.

§ 1 a CoKoBeV vom 26. November 2020

(…)

(3) Die Verpflichtung nach Abs. 1 Satz 1 und 2 besteht nicht für

1. *Kinder unter 6 Jahren,*
2. *Personen, die aufgrund einer gesundheitlichen Beeinträchtigung oder Behinderung keine Mund-Nasen-Bedeckung tragen können,*

3. *Personal von Einrichtungen und Unternehmen nach Abs. 1 Satz 1, soweit kein Kontakt zu anderen Personen besteht oder anderweitige und mindestens gleichwertige Schutzmaßnahmen, insbesondere Trennvorrichtungen, getroffen werden,*
4. *Lehrende an Hochschulen, Berufsakademien, Musikakademien sowie außerschulischen Bildungseinrichtungen und Beteiligte an Prüfungen, wenn ein Hygienekonzept besteht, das zumindest die einzuhaltenden Abstände und den regelmäßigen Luftaustausch sicherstellt,*
5. *Beteiligte an der staatlichen Pflichtfachprüfung und an der zweiten juristischen Staatsprüfung,*
6. *Lehrende und Lernende beim praktischen Unterricht mit Blasinstrumenten, sowie*
7. *Kundinnen und Kunden in Betrieben und Einrichtungen nach Abs. 1 Satz 1 Nr. 4, soweit und solange die Inanspruchnahme der Dienstleistung nur ohne Mund-Nasen-Bedeckung erfolgen kann.*

Rechtliche Bewertung

Bei der Information, ob jemand gesundheitlich beeinträchtigt ist oder eine Behinderung hat und daher keine Mund-Nasen-Bedeckung tragen kann, handelt es sich zweifelsohne um Gesundheitsdaten nach Art. 4 Nr. 15 DS-GVO, bei denen eine Verarbeitung nach Art. 9 DS-GVO nur in sehr eingeschränkten Fällen erlaubt ist.

Zu prüfen ist allerdings auch, ob die DS-GVO überhaupt bei der Prüfung der Befreiung von der Maskenpflicht Anwendung findet. Art. 2 Abs. 1 DS-GVO bestimmt den sachlichen Anwendungsbereich der DS-GVO. Danach gilt die Verordnung für die Verarbeitung von Daten, die in einem Dateisystem gespeichert sind oder werden sollen.

Sofern bei der Prüfung der Maskenpflicht keine Datenverarbeitung, das heißt keine Erfassung oder Speicherung der Informationen erfolgt, fällt die Prüfung der Maskenpflicht durch Ladeninhaber nicht in den Anwendungsbereich des Datenschutzrechts.

Selbst wenn man die Auffassung vertritt, die rein visuelle Prüfung der Maskenbefreiung falle unter die DS-GVO, könnte eine solche Datenerhebung durch den Ladeninhaber nach Art. 9 Abs. 2 i) DS-GVO i. V. m. § 22 Abs. 1 Nr. 1 c) BDSG gerechtfertigt sein. Für eine Speicherung dieser Informationen sehe ich hier allerdings keine Erforderlichkeit.

Fazit und Ausblick

In Zusammenhang mit Geschäften gab es im Berichtsjahr weder in der Corona-Verordnung noch in der Rechtsprechung genaue Hinweise, wie eine Maskenbefreiung nachgewiesen werden kann bzw. welchen Inhalt eine solche Bescheinigung haben muss. Ladenbetreiber können jedoch das Hausrecht

geltend machen und Kunden ohne Maske, die eine Befreiung von der Maskenpflicht nicht glaubhaft machen können, des Geschäfts verweisen. Wann diese Befreiung tatsächlich glaubhaft gemacht wird, ist nicht definiert – und liegt damit letztendlich im Ermessen des jeweiligen Gegenübers.

Aus Datenschutzsicht sind Datenerhebungen beim Betroffenen auf das erforderliche Maß zu beschränken. Wird die Maskenbefreiung durch den Betroffenen gegenüber dem Ladeninhaber mit einem Attest nachgewiesen, ist eine Inaugenscheinnahme ausreichend. Für das Fertigen einer Kopie gibt es allerdings keine hinreichende Rechtsgrundlage.

8.4
Zugriff auf Daten durch ehemaligen Mitarbeiter im Krankenhaus

Scheiden Beschäftigte aus einem Krankenhaus aus, muss darauf geachtet werden, dass ihnen auch der Zugriff auf die Daten des Krankenhauses entzogen wird.

Im letzten Jahr meldete mir ein hessisches Krankenhaus im Rahmen einer Meldung nach Art. 33 DS-GVO folgenden Sachverhalt:

Ein früherer Mitarbeiter, der bereits aus dem Dienst des Krankenhauses ausgeschieden war, wurde dabei gesehen, wie er sich Zugang zu einem Stationsstützpunkt verschaffte und dort an einem Krankenhaus-PC Arbeiten durchführte.

Zum Zeitpunkt der Meldung des Vorfalles konnte nicht ausgeschlossen werden, dass der ehemalige Mitarbeiter Zugriff auf personenbezogene Daten Dritter genommen hatte.

Rechtzeitig innerhalb der Meldefrist von 72 Stunden erfolgte durch das Krankenhaus eine entsprechende Meldung an mich.

Rechtliche Bewertung

Nach Art. 5 Abs. 1 lit. f i. V. m. Art. 32 DS-GVO müssen die Daten im Krankenhaus 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.

Das Krankenhaus muss also dafür sorgen, dass es Unbefugten nicht möglich ist, Zugang zu Patientendaten zu erlangen. Dazu gehört, dass der Zugang zu und der Zugriff auf die Rechner entsprechend gesichert ist. Dies kann entweder durch technische Maßnahmen, wie zum Beispiel einen Passwort-

schutz der PCs, erfolgen oder auch durch organisatorische Maßnahmen, wie zum Beispiel Zutrittsbeschränkungen.

Nach Beendigung des Beschäftigungsverhältnisses darf es daher den ehemaligen Mitarbeitern nicht mehr möglich sein, auf Daten des Krankenhauses Zugriff zu nehmen.

Getroffene Maßnahmen

Nach dem Vorfall hat das Krankenhaus alle Benutzer-Accounts des ehemaligen Mitarbeiters deaktiviert und die Mitarbeiter der Station und der Pforte darüber informiert, dass es sich bei der Person um einen ausgeschiedenen Mitarbeiter handelt.

In der Folge kam es noch zu einer Auswertung durch die IT-Abteilung, um nachzuvollziehen, ob und wenn ja, welche Daten durch den ehemaligen Mitarbeiter eingesehen wurden.

Es stellte sich heraus, dass der bereits ausgeschiedene Mitarbeiter, der im Bereich des Stationsstützpunktes von Mitarbeitern gesehen wurde, auf keine personenbezogenen Daten zugegriffen hatte.

Mittels der Log-Files der Windowssitzungen sowie den Protokollierungsdaten im Krankenhausinformationssystem konnte nachvollzogen werden, dass die letzten Anmeldungen dieses Mitarbeiters vor seinem Austrittsdatum erfolgt sind und kein Zugriff auf Patientendaten erfolgte. Eine Information der Betroffenen nach Art. 34 DS-GVO war dementsprechend nicht erforderlich.

Weiterhin wurden die Mitarbeiter noch einmal darauf hingewiesen, dass Personen, die ihnen nicht bekannt sind und die sich in Bereichen aufhalten, die ausschließlich Mitarbeitern vorbehalten sind, umgehend beim Vorgesetzten und/oder beim Datenschutzbeauftragten zu melden sind.

Fazit

Scheiden Mitarbeiter aus einem Unternehmen aus, darf der Verantwortliche es nicht versäumen, die Accounts der Mitarbeiter zu deaktivieren und ggf. Passwörter zu ändern.

Außerdem zeigt der Fall, wie wichtig und sinnvoll es ist, dass eine entsprechende Protokollierung der Zugriffe erfolgt. Auf diese Weise kann im Einzelfall nachgeprüft werden, ob ein unberechtigter Zugriff auf personenbezogene Daten stattfand.

8.5
Der Anonymitätsgrundsatz im Transplantationsrecht

Im deutschen Transplantationsrecht gilt der Grundsatz der Anonymität zwischen Organspendern bzw. deren Angehörigen und Organempfängern. Auch durch die ausdrückliche Einwilligung der betroffenen Personen kann dieser Grundsatz nicht durchbrochen werden. Zulässig sind Briefwechsel zwischen Angehörigen der Organspender und Organempfänger durch anonymisierte Schreiben.

Ein Angehöriger eines verstorbenen Organspenders beschwerte sich in seiner Eingabe über das Zurückhalten eines Briefes durch die Deutsche Stiftung Organtransplantation (DSO). Die DSO ist die bundesweite Koordinierungsstelle für die postmortale Organspende. Sie erhielt schon 2016 einen Brief eines Organempfängers, der an den Eingebenden gerichtet war.

Die DSO leitete zur dieser Zeit entsprechende Briefe aufgrund der unklaren Rechtslage nicht weiter. Erst nach einer entsprechenden Gesetzesänderung des Transplantationsgesetzes wurden die Briefe anonymisiert und an die Empfänger gesendet. Auch der Eingebende erhielt mit einiger Verzögerung den Brief des Organempfängers. Er hinterfragte in seiner Eingabe unter anderem das Zurückhalten des Briefes und die rechtliche Einschätzung der DSO, dass trotz der entsprechenden Einwilligungen die Aufhebung der Anonymität hier nicht zulässig sei.

Rechtliche Bewertung

Im deutschen Transplantationswesen gilt der Grundsatz der Anonymität zwischen Organspendern bzw. deren Angehörigen und Organempfängern. Im Transplantationsgesetz (Gesetz über die Spende, Entnahme und Übertragung von Organen und Geweben vom 4. September 2007, BGBl. I S. 2206, TPG) ist in § 14 Abs. 2 S. 3 ein striktes Zweckbindungsgebot geregelt:

„Die im Rahmen dieses Gesetzes erhobenen personenbezogenen Daten dürfen für andere als in diesem Gesetz genannte Zwecke nicht verarbeitet werden."

Selbst die Einwilligung der betroffenen Personen kann die Nutzung der Kontaktdaten durch die DSO zu Zwecken des Briefwechsels nicht legitimieren. Nach § 14 Abs. 2 S. 1 TPG dürfen die Mitarbeiter der DSO grundsätzlich keine personenbezogenen Daten von Organspendern, Angehörigen von Or-

ganspendern oder Organempfängern offenbaren. Ein Verstoß gegen dieses strikte Offenbarungsverbot ist strafbar (§ 19 Abs. 3 Nr. 3 TPG).

Daher war das Vorenthalten der Briefe durch die DSO datenschutzrechtlich nicht zu beanstanden. Aufgrund des Anonymitätsgebotes und der strengen Zweckbindung war eine rechtssichere Verwendung der Kontaktdaten selbst für eine anonymisierte Kommunikation nicht möglich.

Erst mit Einführung des neuen § 12a TPG zum 01.04.2019 wurde eine klare gesetzliche Grundlage für die Vermittlung der Briefe zwischen Organempfängern und Angehörigen von Organspendern geschaffen (§ 12a Abs. 1 S. 1 Nr. 4 und 5 TPG). Nach § 12a Abs. 7 TPG muss die Anonymität zwischen Organempfänger und Angehörigen von Organspendern weiterhin sichergestellt werden. Selbst auf ausdrücklichen Wunsch beider Parteien darf die DSO auch nach der neuen Rechtslage keine Kontaktdaten für ein persönliches Treffen oder einen direkten Kontakt offenlegen.

Rechtlicher Hintergrund

Der deutsche Gesetzgeber betrachtet die Anonymität zwischen Organempfängern und Organspendern als einen wichtigen Grundsatz des Transplantationswesens. Die Sicherstellung der Anonymität und das strikte Zweckbindungsgebot sollen nicht nur dem Recht auf informationelle Selbstbestimmung der Betroffenen dienen, sondern auch das Vertrauen der Bevölkerung in die sachgerechte Organempfängerauswahl und die an der Organ- und Gewebespende beteiligten Personen und Institutionen schützen (Spickhoff/Scholz/Middel, 3. Aufl. 2018, TPG § 14 Rn. 1). Der Eindruck einer nicht auf sachlichen Gründen beruhenden Auswahl des Organempfängers soll verhindert werden, auch um die Akzeptanz der Organspende zu erhöhen.

Die Anonymität zwischen Organspendern bzw. deren Angehörigen und Organempfängern ist in vielen europäischen Rechtsordnungen vorgesehen. Auch die Weltgesundheitsorganisation (WHO) erklärt in ihren Richtlinien für die Transplantation menschlicher Zellen, Gewebe und Organe, dass die Anonymität von Organspendern und Organempfängern stets zu schützen ist (WHO, Guiding Principles on Human Cell, Tissue and Organ Transplantation, Guiding Principle 11). Begründet wird dies generell wohl auch mit dem Schutz vor potenziellem Missbrauch oder finanziellem Druck.

Fazit

Ein datenschutzrechtliches Fehlverhalten der DSO lag hier nicht vor. Im Transplantationsrecht gilt der Anonymitätsgrundsatz vorrangig vor der Einwilligung der Betroffenen. Die freiverantwortliche Entscheidungsbefugnis

von Organempfängern und Angehörigen von Organspendern wird dadurch eingeschränkt und die Kommunikation erschwert. Dieser Zustand kann bei den Betroffenen Unverständnis hervorrufen, Abhilfe könnte aber nur eine entsprechende Gesetzesänderung schaffen.

8.6
Datenschutzkonforme Kontrolle und Dokumentation des Masernschutzes

Aus datenschutzrechtlicher Sicht darf die Kontrolle des Masernschutzes grundsätzlich nur durch Vorlage des Impfausweises bzw. der ärztlichen Bescheinigungen erfolgen. Die Anfertigung von Kopien dieser Dokumente ist nicht zulässig, da ein entsprechender interner Aktenvermerk zu Dokumentationszwecken ausreichend ist. Aufgrund des Grundsatzes der Datensparsamkeit sollten der Name des jeweiligen Arztes sowie konkrete Diagnosen nur dann gespeichert werden, wenn triftige Gründe dies erfordern.

1. Hintergrund

Durch das Masernschutzgesetz (BGBl. I 2020 S. 148) wurden Gemeinschaftseinrichtungen – wie Schulen, Kindertagesstätten und Asylbewerberunterkünfte – und medizinische Einrichtungen (im Folgenden zusammen „Einrichtungen“) zum 01.03.2020 verpflichtet, den Masernschutz ihrer Beschäftigten bzw. der von ihnen betreuten Personen zu kontrollieren.

Der Nachweis des Impfschutzes kann nach § 20 Abs. 9 Infektionsschutzgesetz (IfSG) durch Vorlage des Impfausweises oder durch ein ärztliches Attest über den Impfschutz bzw. die Masern-Immunität erbracht werden. Bei einer medizinischen Kontraindikation, die gegen eine Impfung spricht, kann stattdessen ein entsprechendes ärztliches Attest vorgelegt werden.

Zur datenschutzkonformen Gestaltung der von den Einrichtungen gemäß § 20 Abs. 9 IfSG verpflichtenden Kontrolle und der entsprechenden Dokumentation erhielt meine Behörde zahlreiche Anfragen von verschiedenen Beteiligten und Institutionen. Daher habe ich meine Einschätzungen zu diesem Thema in einem Webseite-Beitrag veröffentlicht. Der Beitrag ist unter dem Link *https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/datenschutzkonforme-kontrolle-und* zu finden.

2. Rechtliche Bewertung

Impfausweise und ärztliche Bescheinigungen enthalten nach Art. 9 Abs. 1 DS-GVO besonders geschützte Gesundheitsdaten. Die Verarbeitung dieser Gesundheitsdaten durch die Einrichtungen ist nach Art. 6 Abs. 1 lit. c i. V. m.

Art. 9 Abs. 2 lit. i DS-GVO i. V. m. § 20 Abs. 9 IfSG und § 20 Abs. 1 Nr. 3 HDSIG bzw. § 22 Abs. 1 Nr. 1 lit. c BDSG zulässig.

Die Einrichtungen sind nach § 20 Abs. 9 IfSG gesetzlich dazu verpflichtet, die entsprechenden Gesundheitsdaten zu verarbeiten. § 20 Abs. 9 S. 4 IfSG enthält sogar eine ausdrückliche Verpflichtung zur Übermittlung von personenbezogenen Daten an das Gesundheitsamt, falls der Einrichtung kein entsprechender Nachweis vorgelegt wird. Der Schutz vor den gesundheitlichen Gefahren im Zusammenhang mit der Ausbreitung der hoch ansteckenden Infektionskrankheit Masern stellt im Übrigen ein legitimes öffentliches Interesse im Sinne dieser Normen dar.

Im Beschäftigtenkontext gilt außerdem § 23a IfSG, nach dem der Arbeitgeber unter bestimmten Voraussetzungen den Impf- und Serostatus der Beschäftigten verarbeiten darf.

3. Kontrolle und Dokumentation in der Praxis

Im Rahmen der Kontrolle des Impfstatus sollen aufgrund des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) nur solche personenbezogenen Daten verarbeitet werden, die für die Erfüllung der Pflichten aus dem IfSG erforderlich sind.

Die Anfertigung von Kopien des Impfausweises oder der ärztlichen Bescheinigungen ist in der Regel nicht erforderlich und daher unzulässig. Es sollte vielmehr ein entsprechender Aktenvermerk oder Dokumentationsbogen verwendet werden. Auch die Speicherung des Namens der Ärztin/des Arztes, die/der die Impfungen durchführte, oder der konkreten Diagnose ist nur bei triftigen Gründen gerechtfertigt.

Falls eine fachlich-medizinische Prüfung der Dokumente angezeigt ist, wie insbesondere bei der Prüfung von ärztlichen Attesten durch das zuständige Gesundheitsamt, kann auch die zeitweise Überlassung des Originalattests und die Verarbeitung zusätzlicher Daten datenschutzrechtlich zulässig sein.

Nach § 20 Abs. 9 S. 1 IfSG ist die Leitung der jeweiligen Einrichtung zuständig für die Prüfung der Masernimmunität und trägt dafür die Verantwortung. Sie kann diese Kontrolle aber auch auf Mitarbeiter der Einrichtung delegieren. Die Schulleitung kann z. B. diese Aufgabe auch der Klassenleitung übertragen.

4. Beratungsbeispiel Schule

Zahlreiche Eingaben zur Kontrolle des Masernschutzes bezogen sich auf Schulen als verantwortliche Einrichtungen. In diesem Zusammenhang haben

mich beispielsweise Eltern danach gefragt, wie die Dokumentation durch die Schule erfolgen darf und welche Informationen gespeichert werden dürfen.

Im Schulbereich ist nach meiner Auffassung die Speicherung der Informationen über den Masernschutz in der elektronischen hessischen Lehrer- und Schülerdatenbank LUSD zulässig und gegebenenfalls der Ablage dieser Informationen in der schriftlichen Schülerakte vorzuziehen. Zum Masernschutzstatus der Schüler und Schülerinnen können in der LUSD nur fünf fest definierte Attribute gespeichert werden. Weitere personenbezogenen Daten werden nicht gespeichert. Durch ein entsprechendes Rollen- und Berechtigungskonzept wird sichergestellt, dass nur die jeweilige Schulleitung und besonders ausgewählte Personen Zugriff auf diese Informationen nehmen können. Eine zusätzliche Speicherung in der Schülerakte ist dann nach dem Grundsatz der Datensparsamkeit in der Regel nicht erforderlich. Sollte diese dennoch erfolgen, so sollten die Informationen zum Schutz vor unberechtigtem Zugriff beispielsweise in einem verschlossenen Umschlag oder in einer besonders gekennzeichneten Mappe separat verwahrt werden.

5. Fazit

Durch das Masernschutzgesetz hat der Gesetzgeber unterschiedlichen Einrichtungen Kontrollpflichten im Zusammenhang mit der Maserninfektionsprävention auferlegt. Bei einigen Einrichtungen bestanden zuvor keine vergleichbaren Verfahren und Prozesse im Umgang mit dem Impfstatus bzw. Gesundheitsdaten ihrer Beschäftigten bzw. betreuten Personen. Der Beitrag auf meiner Webseite soll daher auch dazu dienen, den Verantwortlichen im Rahmen der Implementierung und Evaluierung der Kontrollen datenschutzrechtlich Hilfestellung zu geben.

8.7
Patientenakten und Mitarbeiterunterlagen in verlassener Klinik

Die Rechtsträger von Kliniken müssen sicherstellen, dass bei Umzug oder Beendigung des Klinikbetriebes sämtliche Unterlagen mit personenbezogenen Daten aus den Klinikräumen entfernt werden. Der Transport von besonders sensiblen Gesundheitsdaten sollte nur durch entsprechend spezialisierte Transport- oder Umzugsunternehmen erfolgen.

In den letzten Jahren häuften sich Medienberichte über leerstehende Krankenhäuser und Kliniken, die als sogenannte „*lost places*“ im Internet veröffentlicht werden. Diese verlassenen medizinischen Einrichtungen werden als Ausflugsorte für besondere Erlebnisse oder ungewöhnliche Fotomotive be-

worben oder als Ort für Feiern genutzt. Manchmal stoßen die Besucher dabei auch auf zurückgelassene Patientenakten oder gar ein ganzes Aktenarchiv.

Fallbeschreibung

Auch in einer hessischen Klinik, die 2015 ihren Betrieb einstellte, wurden im Sommer 2019 vereinzelte Dokumente aus dem Klinikbetrieb gefunden. Durch einen Artikel auf www.bild.de erfuhr die frühere Klinikbetreibergesellschaft davon. Diese informierte mich darüber durch eine Meldung nach Art. 33 DS-GVO. Um die weitere Offenlegung und Verbreitung von sensiblen personenbezogenen Daten zu verhindern, war ein Besuch der verlassenen Klinik durch meine Mitarbeiter angezeigt. Nachdem der aktuelle Eigentümer kontaktiert wurde und sein Einverständnis gab, machten sich meine Mitarbeiter vor Ort ein Bild von den Gegebenheiten.

Dabei stellten sie fest, dass das Gebäude von außen mit einem Bauzaun umzäunt war und die Fenster im Erdgeschoss sowie der Haupteingang größtenteils von innen verbaut waren. Einige der Fenster im Erdgeschoss waren jedoch eingeschlagen. In dem Klinikgebäude stellten sie unter anderem Mitarbeiterdienstpläne und -telefonlisten, Disketten, ein Patientenrezept, Aktendeckel mit Patientendaten und einen vollständigen Entlassungsbrief sicher. Später wurden auch Röntgenaufnahmen ohne Personenbezug sowie weitere Disketten und Mitarbeiterfotos gefunden.

Nach Angaben von ehemaligen Mitarbeitern der Klinik wurden alle Unterlagen mit personenbezogenen Daten vor Schließung der Klinik organisiert, ordnungsgemäß zusammengepackt und abtransportiert. Die Patientenunterlagen der Klinik, die ca. 1100 Kartons umfassten, wurden fachgerecht von einem Dienstleister eingelagert. Die frühere Klinikbetreibergesellschaft konnte mir dies durch entsprechende Rechnungen und Auftragsunterlagen nachweisen. Außerdem beauftragte sie bis zum Verkauf des Grundstücks einen Sicherheitsdienst mit der Bewachung des Gebäudes.

Daher gehe ich davon aus, dass es sich um vereinzelte Unterlagen und Dokumente handelte, die wohl bei dem Auszug aus dem Gebäude übersehen wurden.

Rechtliche Bewertung

Patientenunterlagen müssen auch nach Schließung einer Klinik aufgrund gesetzlicher (z. B. § 630f Abs. 3 BGB) und berufsrechtlicher Aufbewahrungspflichten sicher verwahrt werden. Die Verantwortlichen müssen nach Art. 5 Abs. 1 lit. f) DS-GVO, insbesondere durch geeignete technische und organisatorische Maßnahmen, eine angemessene Sicherheit personenbezogener

Daten gewährleisten. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt unter anderem von dem Risiko eines unberechtigten Zugriffs, der Art der Verarbeitung sowie der Bedeutung der Daten für die Rechte und Interessen der betroffenen Person ab. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken durch unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten zu berücksichtigen (Art. 32 Abs. 1 und 2 DS-GVO).

Bei Patientenunterlagen handelt es sich um durch Art. 9 Abs. 1 DS-GVO besonders geschützte Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO.

Bei dem Umzug oder der Räumung einer Klinik hat die Betreibergesellschaft daher dafür Sorge zu tragen, dass sämtliche Patientenunterlagen sicher abtransportiert und verwahrt werden. Eine fachgerechte Ausführung dieser Arbeiten, die die Sensibilität der Patientenunterlagen berücksichtigt, kann durch ein entsprechend spezialisiertes Transportunternehmen sichergestellt werden. Das Transportunternehmen ist ausdrücklich auf den besonderen Schutz der Patientendaten hinzuweisen. Im Anschluss an den Abtransport der Patientenunterlagen sollte sich die Betreibergesellschaft selbst davon überzeugen, dass keine Unterlagen mit personenbezogenen Daten zurückgelassen wurden.

Das verlassene Klinikgelände war hier nicht ausreichend gegen unbefugten Zutritt Dritter geschützt. Die Sicherung des Gebäudes unterfiel nicht mehr der Verantwortung der Klinikbetreibergesellschaft, allerdings hätten keine – auch nicht einzelne – Unterlagen mit Patienteninformationen zurückgelassen werden dürfen. Eine besondere Verpflichtung des Transportunternehmens bzw. eine entsprechende Fachkunde wurden mir nicht dargestellt. Eine sorgfältige abschließende Kontrolle der Klinikräume hat ebenfalls nicht stattgefunden.

Verstöße gegen Art. 5 lit. f DS-GVO können nach Art. 83 Abs. 5 a DS-GVO mit einem erhöhten Bußgeld geahndet werden. Aufgrund der rechtzeitigen Meldung nach Art. 33 Abs. 1 DS-GVO war der Sachverhalt für die Krankenhausbetreibergesellschaft hier aber nicht bußgeldrelevant. Die nicht datenschutzkonforme Räumung der Klinik fand auch vor Geltung der DS-GVO statt. Im Übrigen war die Klinikbetreibergesellschaft sehr kooperativ und hat meine Mitarbeiter bei der Bearbeitung des Vorgangs sehr gut unterstützt.

Fazit

Für künftige Umzüge oder Räumungen von Archiven mit Patientenunterlagen oder ganzen Krankenhausabteilungen empfehle ich, ein auf den Umzug von sensiblen Patientendaten spezialisiertes Unternehmen auszuwählen und dafür Sorge zu tragen, dass diese dann auch in geeigneter Weise verwahrt werden.

Zudem sollte auch die Versicherung des Umzugsunternehmens eingeholt werden, dass sämtliche Daten mit Patienten- oder Mitarbeiterbezug aus der Einrichtung entfernt werden, sowie eine abschließende Kontrolle durchgeführt werden. Durch die Berichterstattung der letzten Jahre sind verlassene Kliniken bundesweit in den Fokus der Öffentlichkeit geraten. Die unbefugte Kenntnisnahme von zurückgelassenen Patientenunterlagen müssen die Verantwortlichen bei Schließung bzw. Umzug einer Klinik in jedem Fall wirksam ausschließen, um keine aufsichtsbehördlichen Maßnahmen zu riskieren.

9. Videoüberwachung

9.1
Videoüberwachung in Hotellerie und Gastronomie

Die Videoüberwachung von Ess- und Aufenthaltsbereichen in einer Gaststätte ist im Regelfall datenschutzrechtlich unzulässig. Gleiches gilt neben Café- und Gastronomieflächen in Bäckereien, Tankstellen etc. auch für Hotels, da sich das Verhalten in diesen Bereichen dem Freizeitbereich der Gäste zuordnen lässt, in dem Persönlichkeitsrechte besonders zu schützen sind.

Im Berichtsjahr ist die Anzahl der Beschwerden und Beratungsanfragen im Bereich der Videoüberwachung im Vergleich zu den Vorjahren nochmals angestiegen (s. I 17.2). Dies könnte bei der Videoüberwachung im nachbarschaftlichen Kontext unter anderem darauf zurückzuführen zu sein, dass aufgrund der Corona-Pandemie mehr Menschen von zu Hause arbeiteten bzw. durch Kurzarbeit oder andere Gründe vermehrt zu Hause waren und so eher auf die ein oder andere Kamera im näheren Umfeld aufmerksam wurden oder sich hierdurch gestört fühlten.

Hinsichtlich Videoüberwachung wird in diesem Tätigkeitsbericht exemplarisch ein Fall aus der Hotellerie und des Gastronomiebetriebes vorgestellt. Bereits im vergangenen Bericht habe ich mich mit dieser Problemstellung auseinandergesetzt. Da im Berichtszeitraum Nachfragen und Beschwerden zu diesem Thema ungebrochen hoch sind, wird das Problem nochmals aufgegriffen und vertieft. Zudem wird auf die neu überarbeitete „Orientierungshilfe Videoüberwachung durch nicht-öffentliche-Stellen“ (mit Stand vom 17. Juli 2020, Link: *https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_vü_dsk.pdf*) sowie die Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte Version 2.0, angenommen durch den Europäischen Datenschutzausschuss am 29. Januar 2020 (Link: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_de*), aufmerksam gemacht.

Eine Familie, die Gast eines Hotels war, beschwerte sich über die Videoüberwachung im Frühstücksraum. Aufgrund der Beschwerde wurde das Videoüberwachungssystem des gesamten Hotels überprüft.

Das Hotel wurde um Auskunft nach Artikel 31 DS-GVO i. V. m. § 40 Absatz 4 BDSG gebeten. Dieser Auskunft kam das Hotel umfassend und fristgerecht nach.

Insgesamt waren 16 Kameras sowie eine Kameraattrappe installiert. Bei allen Kameras handelte es sich um sog. Dome-Kameras, deren Schwenk- und Zoomfunktion technisch nicht freigeschaltet und von extern nicht steuerbar war. (Bei einer Dome-Kamera handelt es sich um eine elektronische Kamera, die von einer halbkugelförmigen, durchsichtigen Kunststoffabdeckung umgeben ist.)

Zur Begründung für die angebrachten Kameras wurde angegeben, dass diese zur Wahrung des Hausrechts, zur Verhinderung und Aufklärung von Straftaten, Vandalismus, von Zechprellerei und Einmietbetrug, Diebstählen, Überfällen sowie zur Gewährleistung der Sicherheit der Gäste und Mitarbeiter sowie deren Eigentum installiert waren.

Die Speicherfrist betrug 72 Stunden. Tonaufzeichnungen erfolgten nicht. Lediglich Haustechniker hatten Zugriff auf erhobene und aufgezeichnete Daten. Das Aufzeichnungsgerät war durch eine doppelte Zugangskontrolle – abgeschlossener Schrank in abgeschlossenem Serverraum – gewährleistet.

Die Kameraattrappe war im Restaurant angebracht.

Nach Prüfung der Unterlagen wurde festgestellt, dass gegen die installierten Kameras in Bereichen der Tiefgarage sowie der Anlieferung keine datenschutzrechtlichen Bedenken bestanden. Insgesamt wurden vier Kameras bemängelt. Dies waren zwei Kameras im Bereich Rezeption/Hotellobby sowie eine funktionstüchtige Kamera im Restaurant, und die Kameraattrappe im Restaurant.

Zur Begründung für den nicht-datenschutzkonformen Betrieb wurde Art. 6 Abs. 1 lit. f. Datenschutz-Grundverordnung (DS-GVO) sowie die Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen zugrunde gelegt.

Eine Videoüberwachung von Ess- und Aufenthaltsbereichen in einer Gaststätte ist im Regelfall datenschutzrechtlich unzulässig. Gleiches gilt für Café- und Gastronomieflächen in Hotels. In Sitzbereichen, der Außengastronomie, an der Theke und an einer Bar halten sich Gäste typischerweise über längere Zeit auf, sie essen, trinken und unterhalten sich. Die Rechtsprechung ordnet dieses Verhalten dem Freizeitbereich der Gäste zu (vgl. AG Hamburg, Urteil vom 22.04.2008 – 4 C 134/08). Persönlichkeitsrechte sind hier besonders zu schützen. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Besucher und greift intensiv in deren Rechte ein. In den Ess- und Aufenthaltsbereichen besteht während der Öffnungszeiten auch keine hohe Gefahr für das Eigentum des Hoteliers. Neben den Gästen befindet sich zu diesen Zeiten Personal auf den überwachten Flächen, das bei entsprechenden Vorfällen unmittelbar die Polizei verständigen kann. Bereiche, die zum längeren Verweilen, Entspannen und

Kommunizieren einladen (hierzu zählt auch das Foyer des Hotels), dürfen daher regelmäßig nicht mit Kameras überwacht werden.

Dient eine Überwachung in Ein- und Ausgangsbereichen, Fluren und Treppenhäusern dem Schutz vor Einbrüchen und ist eine Alarmanlage nicht geeignet, wirksam davor zu schützen, dürfen Kameras an dieser Stelle außerhalb der Öffnungszeiten betrieben werden.

Lager und Tresorräume sind in einer Gaststätte / einem Hotel für Gäste üblicherweise nicht frei zugänglich. Sie können überwacht werden, wenn in diesen Bereichen keine dauerhaften Arbeitsplätze eingerichtet sind und keine milderen Mittel zur Zweckerreichung zur Verfügung stehen, beispielsweise den Zutritt nur berechtigten Personen zu ermöglichen. Der Erfassungsbereich der Kamera ist auf das Notwendigste zu beschränken. In Küchen dürfen Kameras nicht eingesetzt werden.

Die Kasse selbst kann während der Öffnungszeiten videoüberwacht werden, wenn Überfälle oder Diebstähle von Dritten verübt wurden und diese ohne Videoüberwachung nicht aufgeklärt oder nachgewiesen werden können. Zudem darf es keine anderen, milderen Maßnahmen zur Sicherung der Kasse geben. Zu prüfen ist, ob die Kasse in einen geschützten Bereich innerhalb der Gaststätte verlegt oder das Kassensystem mit technischen Maßnahmen (Codekarte, Passwort etc.) vor Zugriffen gesichert werden kann. Persönlichkeitsrechte von Beschäftigten sind auch in diesem Bereich zu achten, weshalb eine Kameraerfassung auf das Kassenterminal zu begrenzen ist.

Nach Aufforderung zur Anpassung der Videoüberwachung wurde die vollständige Entfernung der beanstandeten Kameras, auch der Kameraattrappe, nachgewiesen.

9.2
Videoüberwachung eines kostspieligen Denkmals auf einem zentralen städtischen Platz

Die klar begrenzte Videoüberwachung eines kostspieligen Denkmals auf einem öffentlichen Platz kann unter Berücksichtigung und Umsetzung weiterer baulich-organisatorischer Maßnahmen datenschutzaufsichtsbehördlich akzeptiert werden, wenn andere Möglichkeiten ersichtlich und nachvollziehbar nicht in Betracht kommen können.

Im Rahmen einer Beratungsanfrage einer hessischen Stadt wurde ich mit der Fragestellung konfrontiert, ob im Rahmen eines Objektschutzes auf einem zentralen Platz der Stadt ein dort errichtetes Denkmal im Hinblick auf dessen hohe Beschaffungs- und Erhaltungskosten videoüberwacht werden

kann. Weitere ergänzende bauliche Sicherungsmaßnahmen rund um das Denkmal waren zusätzlich bereits konkret ins Auge gefasst worden.

Das von einem Künstler geschaffene Kunstwerk war ca. 140.000 Euro teuer und wurde kurz nach dessen Enthüllung und Öffentlichkeitspräsentation nach nicht einmal einer Woche durch Farbschmierereien (Graffiti) erheblich beschädigt. Hierdurch wurden wegen des für das Kunstwerk verwendeten Materials gleichermaßen aufwändige, langfristige wie kostenintensive Sanierungsarbeiten ausgelöst.

Rechtliche Bewertung

Bei dem hier vorgetragenen Sachverhalt war speziell zu berücksichtigen, dass einerseits ein zentraler und stark besuchter und frequentierter Platz der Stadt angesprochen war und andererseits auch eine große kirchliche Einrichtung sich diesem Platz anschloss bzw. an diesen unmittelbar und „fließend“ angrenzte.

Die Prüfung der Zulässigkeit der Errichtung der hier geplanten Videoüberwachungseinrichtung war hier am Maßstab von Art. 6 Abs. 1 e DS-GVO i. V. m. § 4 HDSIG vorzunehmen.

Nach § 4 Abs. 1 HDSIG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie 1. zur Aufgabenerfüllung öffentlicher Stellen, oder 2. zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 4 Abs. 3 S. 1 HDSIG).

Die Stadt hatte mir zusätzlich zur geplanten Installation einer Videokamera eine weitere vorgreifende Maßnahme dargelegt. Zunächst solle das Denkmal baulich umrandet und eingerahmt werden. Durch die Errichtung eines Zaunes oder einer Mauer solle eine unmittelbare Kontaktmöglichkeit zum Denkmal ausgeschlossen werden. In der Folge solle und könne der Bereich der Videoüberwachung auf diesen umfriedeten, nicht mehr frei zugänglichen Bereich eingeschränkt werden.

Grundsätzlich findet der Besuch eines als Sehenswürdigkeit bekannten öffentlichen Platzes einer Stadt durch Privatpersonen, ein Spaziergang oder auch ein Verweilen hier regelmäßig im Rahmen der individuellen persönlichen Freizeitgestaltung dieser Personen statt. Im Rahmen ihrer Freizeitgestaltung können diese grundsätzlich und vielleicht insbesondere dann, wenn sich hier

angrenzend und in unmittelbarer Sichtnähe eine große kirchliche Einrichtung befindet, davon ausgehen, dass sie sich an diesem Platz unbeobachtet und frei bewegen können, ohne dass eine Videoüberwachung und -aufzeichnung erfolgt.

Zu welcher Uhrzeit, an welchem Tag, in welchem Zustand, mit welchem Erscheinungsbild und wie lange sich eine Person dort aufhält, wie sie diesen Bereich nutzt, wie sie sich dort verhält und ob sie allein oder in Begleitung ist, dies alles würde durch eine den Platz als Ganzes fokussierende Videoaufzeichnung dokumentiert.

Die Stadt hatte genau dies aber nicht im Sinn, sondern nach Abschluss der zunächst vorzunehmenden baulichen Veränderungen (Einfriedung des Denkmals) sollte lediglich nur dieser nicht mehr frei zugängliche und in diesem Sinne dann auch nicht mehr öffentliche Bereich zum alleinigen Objektschutz überwacht werden.

Im Ergebnis der hier vorzunehmenden Interessenabwägung nach § 4 HDSIG war ich in dieser speziellen Fallkonstellation und unter Würdigung und Berücksichtigung der Planungsangaben bereit, in diesem besonderen Einzelfall die Errichtung einer Videoschutzanlage zu akzeptieren. Ich habe jedoch deutlich auf die Voraussetzung hingewiesen, dass sämtliche von der Stadt mir unterbreiteten Vorschläge zwingend einzuhalten sind, namentlich die Errichtung der Anlage allein zum Objektschutz, die Fokussierung der Videokamera einzig und allein auf den dann nicht mehr zugänglichen, umfriedeten Bereich des Kunstwerks und damit einhergehend keinerlei Erfassung von Personen/Passanten am/auf dem Platz.

Fazit

Die anfragende Stadt hat meine rechtliche Einschätzung und Bewertung begrüßt. Darüber hinaus hat sie das geplante Vorgehen und meine Stellungnahme auch mit dem Künstler einerseits und der Kirche andererseits besprochen und abgestimmt, so dass eine für alle involvierten Stellen transparente und konsensuale Lösung gefunden werden konnte.

9.3
Unzulässige Videoüberwachung eines Heimatmuseums

Die flächendeckende Videoüberwachung eines kleinstädtischen Heimatmuseums während dessen Öffnungszeiten lässt sich, auch wenn einige kleinere Diebstähle erfolgt sind, wegen der Unverhältnismäßigkeit einer solchen Maßnahme nicht rechtfertigen. Das Interesse von Besucherinnen und Besuchern an einem ungestörten, d. h. unbeobachteten Aufenthalt im

Rahmen ihrer persönlichen Freizeitgestaltung überwiegt das Interesse der Kleinstadt.

Mich erreichte eine Beratungsanfrage einer hessischen Kleinstadt zur Möglichkeit, das dortige städtische Heimatmuseum flächendeckend in allen Räumlichkeiten mit einer Videoüberwachungsanlage auszurüsten. Hintergrund dieses Wunsches war die Verzeichnung einiger Diebstähle (Kartenständer, Diorama) oder vereinzelter Vandalismus an Ausstellungsgegenständen.

Das Gebäude wurde mir als dreigeschossig mit einer Gesamtfläche von über 500 m^2 beschrieben. Das Heimatmuseum sei an fünf bis sechs Tagen im Monat geöffnet und werde durch einen dortigen Museumsverein ehrenamtlich – auch während der Öffnungszeiten – betreut. Zusätzlich würden die Räumlichkeiten auch regelmäßig für Vorträge sowie als Wahllokal genutzt.

Man plane die Errichtung einer Videoüberwachungseinrichtung in allen Ausstellungsräumen, in denen rund um die Uhr Videoaufzeichnungen mit einer Speicherdauer von sieben Tagen erfolgen sollen. Lediglich bei Vorträgen und Wahlen plane man, in den jeweiligen Räumlichkeiten zu diesen Anlässen die jeweiligen Videokameras abzudecken. Über ein noch zu präzisierendes Zugriffskonzept auf die gespeicherten Aufzeichnungen habe man sich erste Gedanken gemacht.

Rechtliche Bewertung

Wie ich seit vielen Jahren regelmäßig in meinen Tätigkeitsberichten betone und immer wieder verdeutlichen muss, stellt eine Videoüberwachung grundsätzlich einen erheblichen Eingriff in das Persönlichkeitsrecht der hiervon Betroffenen dar und kann somit eine Persönlichkeitsrechtsverletzung sein. Die Gefahr der Einflussnahme auf das Verhalten der Betroffenen und dessen Lenkung ist einer Videoüberwachungseinrichtung immanent.

Die Prüfung der Zulässigkeit der Errichtung einer solchen Videoüberwachungseinrichtung war vorliegend mit Blick auf den verantwortlichen Betreiber – entweder der Museumsverein oder die Stadt – zweifach zu prüfen. Für den Museumsverein als Verantwortlichen ist die Prüfung grundsätzlich am Maßstab des Art. 6 Abs. 1 lit. f DS-GVO vorzunehmen, für die hessische Kleinstadt ist Art. 6 Abs. 1 lit. e DS-GVO i. V. m. § 4 HDSIG mögliche Gesetzesgrundlage.

Nach Art. 6 Abs. 1 lit. f DS-GVO ist eine Datenverarbeitung nur rechtmäßig, wenn die Verarbeitung 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.

Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen (ErwGr. 47 zur DS-GVO).

Nach § 4 Abs. 1 HDSIG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie 1. zur Aufgabenerfüllung öffentlicher Stellen, 2. zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (§ 4 Abs. 3 S. 1 HDSIG).

Die Stadt hatte als Anlass für die Errichtung einer Videoüberwachungsanlage neben den bereits oben erwähnten Hintergründen zusätzlich noch angegeben, dass die Räumlichkeiten nur schwer einzusehen seien und in der Regel nur durch eine (ehrenamtliche) Aufsicht im Eingangsbereich während der Öffnungszeit überwacht würden.

Der Besuch eines kleinstädtischen Heimatmuseums findet regelmäßig im Rahmen der individuellen persönlichen Freizeitgestaltung statt. Im Rahmen dieser Freizeitgestaltung können vorliegend Personen vernünftigerweise und grundsätzlich davon ausgehen, dass diese in einem kleinstädtischen Museum unbeobachtet stattfindet, insbesondere ohne Videoüberwachung und -aufzeichnung.

Zu welcher Uhrzeit, an welchem Tag, in welchem Zustand, mit welchem Erscheinungsbild und wie lange sich eine Person dort aufhält, wie sie diesen Bereich nutzt, wie sie sich dort verhält und ob sie allein oder in Begleitung ist, dies alles wird gerade und insbesondere durch eine Videoaufzeichnung dokumentiert. Wie lange sich aber Personen während der Öffnungszeiten tatsächlich in den Räumlichkeiten aufhalten und vor den unterschiedlichen Ausstellungsstücken und Exponaten verweilen, müssen diese frei entscheiden können. Darüber hinaus gibt auch der ganz überwiegende Großteil der Besucherinnen und Besucher keinerlei Anlass für die Notwendigkeit einer Dauerüberwachung mittels Videokameras.

Im Ergebnis der hier vorzunehmenden Interessenabwägung sowohl nach Art. 6 Abs. 1 lit. f DS-GVO als auch nach § 4 HDSIG überwiegen während

der regulären Öffnungszeiten des Museums die (berechtigten) Interessen der Museumsbesucherinnen und -besucher an einem ungestörten, freien Museumsbesuch, bei dem sie sich nicht filmen lassen müssen, diejenigen Interessen der Stadt, der zur Sicherung des Inventars oder zum Schutz vor Vandalismus andere Möglichkeiten zur Verfügung stehen, die nicht in die Grundrechte der Besucherinnen und Besucher eingreifen. So kommen hierfür z. B. abschließbare Vitrinen (mit Sicherheitsglas), die feste technische Fixierung einzelner Gegenstände an Wänden/im Boden oder die Anbringung von Schutzabdeckungen vor ausgestellten Dokumenten als mildere Maßnahmen in Betracht.

Die Möglichkeit einer Videoüberwachung besteht allenfalls nur außerhalb der Öffnungszeiten des städtischen Museums.

Fazit

Ich habe der anfragenden Kleinstadt meine rechtliche Einschätzung und Bewertung dargelegt. Für die von dort gewünschte Installation einer Videoüberwachungsanlage im Heimatmuseum besteht während der Öffnungszeiten keine Möglichkeit. Dieses Ergebnis wurde von der Stadt akzeptiert; jedenfalls liegen mir keine anderen Informationen vor.

10. Vereine

10.1
Vorsorgliche Erhebung von Gesundheitsdaten durch den Sportverein im Zeichen der Corona-Pandemie

Für die Erhebung von Gesundheitsdaten durch Sportvereine im Rahmen des Trainings- oder Wettkampfbetriebes ergibt sich keine spezifische Rechtsgrundlage. Es gilt vielmehr Art. 6 Abs.1 lit. a, f DS-GVO. Dabei haben sich die Sportvereine stets am Grundsatz von Verhältnismäßigkeit und Erforderlichkeit zu orientieren. Ich habe die Vereine zu einem frühen Zeitpunkt über meine Rechtsauffassung informiert und eine Handlungsanleitung auf meiner Homepage veröffentlicht.

Nach dem ersten Lock-Down erreichten mich Anfragen aus der Vereinslandschaft, aber auch Beschwerden von Eltern, deren Kinder Fragen zum aktuellen Gesundheitsstatus beantworten sollten, um am Trainingsbetrieb im Verein teilnehmen zu können. Dabei ging es um Fragestellungen wie z. B. „Hast Du Schnupfen oder Husten?“, „Hast Du Fieber?“ oder „Warst Du im Urlaub in einem Risikogebiet?“. Mit diesen Momentaufnahmen waren Vereine bemüht, mögliche Infektionsherde im Trainingsbetrieb nicht entstehen zu lassen bzw. aus einer drohenden Haftung herauszunehmen.

An einer Rechtsgrundlage für die Datenerhebung mangelt es

Im Rahmen meiner Ermittlungen nahm ich mit dem Landessportbund Hessen (lsbh) Kontakt auf. Dieser verwies auf eine Veröffentlichung des Deutschen Olympischen Sportbundes, der in einem „Leitplanken-Papier“ Empfehlungen für die Einhaltung von Distanzregeln erarbeitet hatte, das aber keine Aussage zur Erhebung von Gesundheitsfragen enthielt. Auch die Verordnung über Kontaktbeschränkungen der Landesregierung enthielt hierzu keine Regelung, sondern verwies auf die Spitzenverbände des Sports.

Fragen zur Gesundheit sind Fragen zu Daten der besonderen Kategorien im Sinne von Art. 9 Abs. 1 DS-GVO, deren Verarbeitung zunächst grundsätzlich untersagt ist und nur aufgrund der Ausnahmeregelung nach Art. 9 Abs. 2 DS-GVO zulässig sein kann. Hier könnte man argumentieren, dass im Sinne von Art. 9 Abs. 2 lit. i DS-GVO „die Verarbeitung für Zwecke der Gesundheitsvorsorge … erforderlich ist“. Dieser Position vermochte ich mich nicht anzuschließen, da ich erhebliche Zweifel an dem Nutzen der Datenverarbeitung und insoweit bereits an der Erforderlichkeit der Erhebung der Daten hatte. Selbst das Robert-Koch-Institut hatte in einer seiner zahlreichen Erklärungen zu Covid 19 verlautbaren lassen, dass die Erhebung solcher

Daten aus medizinischer Sicht nicht erheblich sei. Ich habe deshalb einer Datenerhebung zur Gesundheit der Vereinsmitglieder widersprochen. Etwas anderes gilt für die Erhebung von Kontaktdaten (Name, Erreichbarkeit) im Rahmen des Trainingsbetriebes. Hier war zu berücksichtigen, dass z. B. im Falle einer SARS-CoV-2-Infektion einer Person, die an einem Sporttraining teilnahm, eine Nachverfolgung der Infektion durch die Gesundheitsämter ermöglicht werden oder potenzielle Gefährdete über eine mögliche Ansteckung mit der Erkrankung informiert werden sollten.

Auf meiner Homepage ist ein Leitfaden veröffentlicht

Der Leitfaden auf meiner Homepage (*https://datenschutz.hessen.de*) beantwortet die diesbezüglichen Fragen der Vereine:

1. Es gibt derzeit keine gesetzliche Verpflichtung, für den Trainingsbetrieb „Corona-Listen“ zu führen. Insoweit bleibt es grundsätzlich dem Verein überlassen, ob er derartige Listen erstellen will oder darauf verzichtet.
2. Sofern der Verein sich jedoch entscheidet, die Trainingsbeteiligung personenbezogen zu dokumentieren, benötigt er eine Rechtsgrundlage für die Datenerhebung (Erstellung und Speicherung Liste) oder die Einwilligung der Betroffenen. Dann sind Erhebungszweck, wie z. B. die Möglichkeit der Nachverfolgung im Falle einer SARS-CoV-2-Infektion, Umfang der Erhebung und Dauer der Speicherung, zu erläutern.
   Eine Rechtsgrundlage ergibt sich aus Art. 6 Abs. 1 lit. f DS-GVO. In diesem Fall kann auf die Einholung einer Einwilligung (Art. 6 Abs. 1 lit. a DS-GVO) verzichtet werden.
3. Streng auszurichten hat sich der Verein auf die Grundsätze von Erforderlichkeit und Verhältnismäßigkeit beim Umfang der zu erhebenden und zu speichernden Daten. Das heißt, dass nur die für den Erhebungs- und Speicherzweck notwendigen Daten abgefragt werden dürfen. Diese sind:
   – Name und Vorname
   – Tag des Trainings
   – Ort des Trainings
   – Kontaktdaten (z. B. Telefonnummer oder E-Mail-Adresse)

   Keinesfalls dürfen also Gesundheitsdaten erfasst werden wie z. B. in der Form, dass man Kinder und Jugendliche nach Krankheitssymptomen befragt und dies dokumentiert. Gleiches gilt für die Erwachsenen.
4. Der Umgang mit den Daten, unabhängig ob analog oder digital, hat sorgfältig und streng zweckgebunden zu erfolgen. Die Listen sind vor dem Zugriff unbefugter Dritter zu schützen.

5. Die Aufbewahrung (Speicherfrist) soll den Zeitraum von einem Monat nicht überschreiten. Digitale Daten sind datenschutzgerecht zu löschen. Gleiches gilt für die Entsorgung bzw. Vernichtung von papiergebundenen Daten.
6. Jeder Verein ist aufgefordert, seine Mitglieder bzw. die Eltern von minderjährigen Mitgliedern über seine Vorgehensweise zu informieren.

Die Vereine haben diese Hinweise des HBDI in der Folge überwiegend dankbar aufgenommen und im Trainingsalltag umgesetzt.

Damit konnte sowohl dem Infektionsschutz, mit der Nachvollziehbarkeit von Infektionsketten durch das Gesundheitsamt, als auch dem Datenschutz Rechnung getragen werden.

10.2
Offenlegung der Mitgliederliste eines Lohnsteuerhilfevereins gegenüber der Oberfinanzdirektion

Im Berichtsjahr trat ein Lohnsteuerhilfeverein mit der Frage an mich heran, ob das Verlangen der Oberfinanzdirektion (OFD) auf Herausgabe einer Mitgliederliste den datenschutzrechtlichen Regelungen entspricht.

Die OFD forderte den Verein auf, seine Mitgliederliste herauszugeben. Darin sind Name und Anschrift sämtlicher Mitglieder enthalten, die zu der Mitgliederversammlung des Vereins geladen waren. Anhand der Liste wollte die OFD kontrollieren, ob die Mitglieder des Vereins ordnungsgemäß zu dessen Mitgliederversammlung geladen waren. Der Verein hatte erhebliche datenschutzrechtliche Bedenken, die geforderte Liste an die OFD zu übergeben. Die Verantwortlichen seitens des Vereins sahen in der von der OFD gewünschten Vorgehensweise einen Verstoß gegen die DS-GVO. Die Übermittlung der gewünschten Daten an die OFD sei von keiner Rechtsgrundlage gedeckt. Die Mitglieder hätten zwar gegenüber dem Verein eine „Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten“ abgegeben, aber auch diese sehe eine solche Übermittlung nicht vor.

Die OFD als Aufsichtsbehörde

Wie sich im Rahmen meiner weiteren Recherche herausstellte, erfolgte die Datenanforderung im Rahmen der aufsichtsrechtlichen Tätigkeit der OFD. Diese führt nach § 27 Abs. 1 Steuerberatungsgesetz (StBerG) die Aufsicht über diejenigen Lohnsteuerhilfevereine, die ihren Sitz im Bezirk der Aufsichtsbehörde haben. Dabei ist die Aufsichtsbehörde zur umfassenden Aufsicht

verpflichtet und befugt. Die Aufsicht umfasse demnach die gesamte fachliche Betätigung, die satzungsgemäße Geschäftsführung des Vereins sowie die Überwachung der Einhaltung sämtlicher für den Lohnsteuerhilfeverein geltenden Vorschriften (§§ 13 ff. StBerG). Auch die DS-GVO stehe einer Übermittlung der Mitgliederliste nicht entgegen. Soweit es zur Erfüllung der aufsichtsrechtlichen Aufgaben der OFD nach dem Steuerberatungsgesetz erforderlich sei, dürften, nach Ansicht der OFD, personenbezogene Daten erhoben und auch für Zwecke künftiger Verfahren verarbeitet und genutzt werden.

Im konkreten Fall verfolgte die Aufforderung durch die OFD den Zweck nachzuvollziehen, ob alle Mitglieder des Lohnsteuerhilfevereins regelmäßig zu den Mitgliederversammlungen eingeladen wurden. Durch die Möglichkeit zur Teilnahme an den Mitgliederversammlungen werden die Mitglieder in die Lage versetzt, ihre Rechte im Verein auszuüben. Zur Prüfung, ob die gem. § 29 Abs. 1 StBerG erforderliche Versammlung durch den Verein tatsächlich durchgeführt wurde, wurde die OFD tätig. Die Rechtsgrundlage hierfür ergibt sich aus § 93 Abs. 1 Satz 1 Abgabenordnung (AO) i. V. m. § 164a StBerG. Danach gehört es zur Aufgabenstellung der Steuerbehörde, zur Prüfung des Sachverhaltes beim Vorstand des Lohnsteuerhilfevereins eine Liste, aus der die Namen und Anschriften der Mitglieder des Lohnsteuerhilfevereins hervorgehen, anzufordern.

Aufforderung zur Herausgabe der Liste ist in dem vorliegenden Fall datenschutzrechtlich zulässig

Im Ergebnis ist die Anforderung einer Liste der Mitglieder des Lohnsteuerhilfevereins durch die OFD datenschutzrechtlich zulässig, da dies auf Grundlage einer gesetzlichen Norm erfolgt. Im Übrigen ist in § 27 StBerG geregelt, dass die jeweils zuständige Landesfinanzbehörde die Aufsicht über die Lohnsteuerhilfevereine hat. Der Bundesfinanzhof fasst die Reichweite dieser Aufsicht weit: „Die Aufsicht erstreckt sich darauf, dass die Vereine die ihnen durch das StBerG in den §§ 21 bis 26 auferlegten Pflichten erfüllen sowie dass sie alle weiteren einschlägigen Vorschriften … beachten“ (BFH, Urteil vom 23. März 1999 – VII R 19/98). Zu den „weiteren einschlägigen Vorschriften“ dürften auch die vereinsrechtlichen Regeln des Bürgerlichen Gesetzbuches sowie der Satzung des Vereins über Mitgliederversammlungen zählen.

Verhältnismäßigkeit und Erforderlichkeit

Dennoch muss sich die Maßnahme der Finanzbehörde am Grundsatz der Verhältnismäßigkeit ausrichten. Insbesondere muss die jeweils konkret in Rede stehende Maßnahme im Einzelfall erforderlich sein. Den Grundsätzen der Verhältnismäßigkeit und Erforderlichkeit schien mir im vorliegenden Sachverhalt durch die Finanzbehörde Rechnung getragen zu sein.

11. Wirtschaft, Banken, Selbstständige

11.1
Übermittlung personenbezogener Daten im Rahmen eines Forderungsverkaufs durch eine Bank an ein Inkasso-Unternehmen

Die Übermittlung von Forderungsdaten an ein Inkasso-Unternehmen ist durch eine Bank in ihrer Eigenschaft als Verkäuferin einer Forderung nach Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 402 BGB zulässig. Eine Einwilligung in die Datenübermittlung durch die Betroffenen ist hierbei nicht erforderlich.

Im Berichtsjahr sind in meiner Dienststelle vermehrt Eingaben bezüglich der Frage der Zulässigkeit von Datenübermittlungen bei Forderungsverkäufen eingegangen.

In allen Fällen war eine Bank, deren eigene Beitreibungsversuche erfolglos geblieben waren, Gläubigerin einer vom Kunden nicht beglichenen Forderung. Daher entschieden sich die Banken in einigen mir zur Kenntnis gebrachten Fällen, die jeweiligen Forderungen an Dritte, die auf die Verwertung von Forderungen spezialisiert sind, zu verkaufen. Da die Forderungsdaten personenbezogene Daten im Sinne der DS-GVO darstellen und diese an Dritte, hier den jeweiligen Forderungskäufer, übermittelt wurden, war zu prüfen, ob diese Datenübermittlung rechtmäßig war.

Datenschutzrechtlich ist eine Übermittlung von personenbezogenen Daten dann rechtmäßig, wenn diese auf eine Rechtsnorm gestützt werden kann. Art. 6 Abs. 1 DS-GVO definiert die Voraussetzungen, die erfüllt sein müssen, damit die Übermittlung von personenbezogenen Daten rechtmäßig ist.

Art. 6 Abs. 1 DS-GVO

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.

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

In den mir zur Prüfung vorgetragenen Fällen ging es um den Verkauf von offenen Forderungen und der damit einhergehenden Übermittlung der personenbezogenen Daten der jeweiligen Schuldner an den Forderungskäufer. Die Bank ist grundsätzlich dazu berechtigt, im Rahmen einer unternehmerischen Entscheidung festzulegen, dass sie Forderungen nicht selbst beitreibt, sondern diese an einen Dritten verkauft. Der Forderungsverkauf selbst stellt einen Rechtskauf nach § 453 BGB dar. Aus dieser vertraglichen Konstellation erwächst seitens des Forderungskäufers ein Anspruch auf Übertragung der Forderung gem. §§ 398 ff. BGB und auf Übermittlung der Forderungsdaten durch den Verkäufer gem. § 402 BGB, damit er die Forderung gegenüber dem Schuldner geltend machen kann.

§ 402 BGB

Der bisherige Gläubiger ist verpflichtet, dem neuen Gläubiger die zur Geltendmachung der Forderung nötige Auskunft zu erteilen und ihm die zum Beweis der Forderung dienenden Urkunden, soweit sie sich in seinem Besitz befinden, auszuliefern.

Nach § 402 BGB ist somit der bisherige Gläubiger (Forderungsverkäufer, hier die Bank) dazu verpflichtet, dem neuen Gläubiger (Forderungskäufer, hier das Inkasso-Unternehmen) die entsprechenden Forderungsdaten und erforderlichen Unterlagen zu übermitteln.

Da es sich hierbei um eine gesetzliche Pflicht handelt, kann somit die Datenübermittlung auf die Regelungen des Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 402 BGB gestützt werden. Folglich ist auch eine Einwilligung in die Übermittlung seitens des Betroffenen nicht erforderlich.

11.2
Verwendung von Mitgliederdaten von Genossenschaftsbanken durch ein Genossenschaftsmitglied

Genossenschaftsmitglieder dürfen die ihnen von der Bank übermittelten Daten anderer Genossenschaftsmitglieder zweckgebunden verarbeiten. Ein Anspruch auf eine vorzeitige Löschung kann seitens der Bank nicht geltend gemacht werden.

Im Berichtszeitraum hat sich eine Genossenschaftsbank an mich gewandt und um Unterstützung bei der Durchsetzung eines Löschungsersuchens gegenüber einem Genossenschaftsmitglied gebeten. Das Mitglied hatte seinerzeit die Volksbank um Herausgabe der Daten der Genossenschaftsmitglieder (Namen und Anschriften) gebeten, um diese über seine Auffassung bezüglich einer möglichen Fusion der Bank mit einem anderen Institut informieren zu können. Die Bank hat daraufhin die Daten dem Mitglied entsprechend zur Verfügung gestellt. Mehrere Monate nach Erhalt der Daten hatte das Mitglied diese allerdings noch nicht verwendet, so dass die Bank nunmehr forderte, diese Daten zu löschen.

Der Aufforderung kam das Mitglied allerdings nicht nach, weshalb die Bank sich an meine Behörde gewandt hat.

Einleitend ist festzustellen, dass die Übermittlung der in Rede stehenden Daten sowohl auf die Regelungen aus § 31 Genossenschaftsgesetz (GenG) als auch auf die Satzung der Bank gestützt werden konnte.

§ 31 GenG

(1) Die Mitgliederliste kann von jedem Mitglied sowie von einem Dritten, der ein berechtigtes Interesse darlegt, bei der Genossenschaft eingesehen werden. Abschriften aus der Mitgliederliste sind dem Mitglied hinsichtlich der ihn betreffenden Eintragungen auf Verlangen zu erteilen.

(2) Der Dritte darf die übermittelten Daten nur für den Zweck speichern und nutzen, zu dessen Erfüllung sie ihm übermittelt werden; eine Speicherung und Nutzung für andere Zwecke ist nur zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen. Ist der Empfänger eine nicht öffentliche Stelle, hat die Genossenschaft ihn darauf hinzuweisen; eine Speicherung und Nutzung für andere Zwecke bedarf in diesem Fall der Zustimmung der Genossenschaft.

Die Datenübermittlung durch die Bank an das Genossenschaftsmitglied war daher nach Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 1 lit. b, c DS-GVO rechtmäßig. Zwischen der Bank und dem Mitglied bestand ein Mitgliedschaftsverhältnis, das dem Mitglied bestimmte satzungsmäßige Rechte zugesteht, u. a. die

Mitgliederliste einzusehen. Zusätzlich gab es auch eine eindeutige gesetzliche Regelung im GenG.

Der Empfänger gab an, die Daten nutzen zu wollen, um die anderen Genossenschaftsmitglieder schriftlich von einer seiner Meinung nach erforderlichen Satzungsänderung zu überzeugen.

Da die anderen Mitglieder auch nach mehr als vier Monaten nach Erhalt der Daten nicht kontaktiert wurden, verlangte die Bank die Löschung der in Rede stehenden Daten vom Mitglied. Dieses wurde seitens des Empfängers mit der Begründung zurückgewiesen, dass es ihm bis dato nicht möglich gewesen sei, die Schreiben zu versenden. So habe die Bank ihm zwar eine Abschrift der Mitgliederliste zur Verfügung gestellt, diese aber nicht in einem gängigen Format übermittelt, so dass die Daten der rund 21.000 Mitglieder manuell für den Versand zu formatieren waren.

Datenschutzrechtlich bestand somit ein Löschanspruch gegenüber dem Mitglied nicht. Nach Art. 5 Abs. 2 DS-GVO müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke verwendet werden. Es war vorliegend nicht ersichtlich, dass der Empfänger die in Rede stehenden Daten zu einem anderen Zweck verarbeiten würde als ursprünglich vom Mitglied angegeben. Daher wurde das Ersuchen der Bank vorliegend zurückgewiesen, da die Datenverarbeitung rechtmäßig war.

11.3
Schwärzungen auf Unterlagen, die von einem Kreditinstitut angefordert wurden

Fordert ein Kreditinstitut von einem Kunden Unterlagen an, können darauf nur in Einzelfällen Schwärzungen vorgenommen werden. Auf Kopien von zur Identifikation vorgelegten Ausweispapieren dürfen Schwärzungen grundsätzlich nicht vorgenommen werden.

Mich erreichen immer wieder Beschwerden, dass Schwärzungen auf Unterlagen, die von Kreditinstituten angefordert und diesen daraufhin in Kopie übergeben wurden, nicht akzeptiert werden. Hierbei ist zunächst zu unterscheiden zwischen Ausweiskopien, die zur Überprüfung der Identität erstellt oder angefordert werden, und sonstigen Unterlagen.

Kreditinstitute sind gemäß §§ 10 Abs. 1 Nr. 1, 11 Abs. 1 Satz 1 Geldwäschegesetz (GWG) verpflichtet, Vertragspartner, Vertretungsberechtigte und wirtschaftlich Berechtigte zu identifizieren. Vertragspartner ist grundsätzlich jeder Kunde eines Kreditinstituts. Wirtschaftlich Berechtigte sind Personen, welche die Kontrolle über Vermögenswerte tatsächlich ausüben. Zur

Identifizierung sind Vorname und Nachname, Geburtsort, Geburtsdatum, Staatsangehörigkeit und eine Wohnanschrift festzustellen und aufzuzeichnen. Die Identifizierung von Personen erfolgt gem. § 12 Abs. 1 Satz 1 Nr. 1 GWG normalerweise durch Vorlage eines gültigen amtlichen Ausweises mit Lichtbild oder ähnlichen Unterlagen.

Zur Dokumentation der Identifizierung sind Kreditinstitute berechtigt und verpflichtet, eine Kopie der vorgelegten Dokumente anzufertigen und aufzubewahren. Diese Verpflichtung ergibt sich aus § 8 Abs. 3 Satz 2 GWG. Die Verarbeitung der erhobenen Daten ist aufgrund der gesetzlichen Verpflichtung zulässig gem. Art. 6 Abs. 1 lit. c DS-GVO.

Da sich die Verpflichtung zur Identifizierung nur auf die im Gesetz genannten Merkmale erstreckt und insbesondere nicht in einem Ausweis typischerweise enthaltene persönliche Merkmale wie Augenfarbe oder Größe umfasst, wurde früher teilweise angenommen, dass Daten auf Kopien, deren Erfassung nicht erforderlich ist, geschwärzt werden dürfen. Auf diese Diskussionen hat der Gesetzgeber mit der Klarstellung im GWG reagiert und geregelt, dass von Ausweisdokumenten „vollständige“ Kopien erstellt werden dürfen und müssen. Diese Klarstellung hat dazu geführt, dass einheitlich die Möglichkeit zur Schwärzung auf Kopien von Ausweiskopien abgelehnt wurde. Zwar ist durch erneute Änderungen im GWG das Wort „vollständig“ wieder entfallen. Daraus ergibt sich jedoch nicht die Möglichkeit, nun wieder Schwärzungen vorzunehmen. Eine entsprechende Änderung wollte der Gesetzgeber nicht durchführen.

Darüber muss die Kopie eines Dokuments grundsätzlich unverfälscht sein. Würde die Kopie Schwärzungen enthalten, würde es sich um eine insoweit zumindest veränderte Kopie des Originaldokuments handeln.

Schwärzungen an Ausweisdokumenten, die zur Identifizierung vorgelegt und zur Dokumentation der Identifizierung kopiert werden, sind daher grundsätzlich nicht zulässig.

Andere Dokumente, die von Kreditinstituten angefordert werden, sind individuell zu betrachten. Eine gesetzliche Verpflichtung zur Anfertigung von Kopien dieser Dokumente besteht grundsätzlich nicht. Daher kann die Verarbeitung der erfassten Daten häufig nur aufgrund eines berechtigten Interesses eines Kreditinstitutes gemäß Art. 6 Abs. 1 lit. f DS-GVO zulässig sein. Hierbei ist individuell zu prüfen, ob ein Kreditinstitut ein berechtigtes Interesse an der Anfertigung oder Überlassung ungeschwärzter Kopien hat, das von den Interessen und Freiheitsrechten betroffener Personen nicht überwogen wird.

Ein berechtigtes Interesse kann sich aus einer Bonitätsprüfung aufgrund des mit einem Kredit eingegangenen Risikos ergeben. Wird von einem

Kreditinstitut ein Kredit gewährt, ist dieses grundsätzlich berechtigt, die Risiken, die sich aus der Rückzahlung des Kredites ergeben, zu überprüfen. Hierfür darf ein Kreditinstitut in der Regel Unterlagen zum Einkommen und der Vermögenssituation anfordern. Derartige Unterlagen können häufig nur im Zusammenhang beurteilt werden. Schwärzungen auf diesen Unterlagen können nicht immer als unbedenklich erkannt werden, wenn der Inhalt des geschwärzten Feldes oder der Inhalt der Schwärzung unbekannt ist. Unterlagen sind auch selten so stark standardisiert, dass bereits aus der Lage der Schwärzung auf der Unterlage deren Unbedenklichkeit erkennbar wäre. Dies gilt insbesondere für Gehaltsabrechnungen, bei denen viele Bestandteile zur Prüfung der Plausibilität der gesamten Unterlage erforderlich sind.

Daher ergibt sich aus einer Abwägung häufig, dass ein Kreditinstitut ein Interesse an der Überlassung ungeschwärzter Kopien hat, um die Authentizität und Echtheit des kopierten Dokumentes überprüfen zu können. In Einzelfällen hat sich jedoch in Beschwerdeverfahren die Unzulässigkeit der Anforderung von ungeschwärzten Kopien ergeben.

Dies war zum Beispiel der Fall bei der Überlassung von Kopien von Mietverträgen, deren Ertrag als Einkommensnachweis diente, ohne dass die betroffene Immobilie als Sicherheit für einen gewährten Kredit dienen sollte. In diesem Fall war zusätzlich zu berücksichtigen, dass es sich dabei um Daten Dritter handelte, die von dem Vertragsverhältnis zwischen dem Kunden und dem Kreditinstitut nicht betroffen waren. Ein Interesse des Kreditinstitutes an dem Inhalt des Mietvertrages war zwar anzuerkennen, dieses umfasste jedoch nicht das Interesse an der Kenntnis des Namens einzelner Mieter. Deren Rechte an dem Unterlassen einer Datenverarbeitung überwogen daher das Interesse des Kreditinstitutes an der Kenntnis dieser Daten. Insoweit war deshalb die betroffene Person zur Schwärzung der Namen berechtigt.

Sofern jedoch die Rechte aus einem abgeschlossenen Mietvertrag als Sicherheit für einen gewährten Kredit dienen, ist auch eine andere Beurteilung möglich. Dies gilt insbesondere dann, wenn die Rechte auf Zahlung des Mietzinses sicherungshalber an ein Kreditinstitut abgetreten werden.

In einem anderen Fall wollte ein Kreditkartenunternehmen ungewöhnliche Zahlungsvorgänge mit der ausgegebenen Kreditkarte durch Einsicht in die ungeschwärzten Kontoauszüge eines Girokontos ihres Kunden überprüfen. Das Kreditkartenunternehmen befürchtete ein erhöhtes Risiko, weil die Zahlungsvorgänge typisch für die Vorbereitung eines Betruges seien. In diesem Fall standen dem Kreditkartenunternehmen aber andere und naheliegendere Möglichkeiten zur Risikobegrenzung oder -vermeidung zur Verfügung. Auch zur Prüfung, ob ein Sachverhalt vorliegt, der auf Geldwäsche oder eine ihrer Vortaten hindeutet oder auf Terrorismusfinanzierung hindeutende

Auffälligkeiten oder Ungewöhnlichkeiten enthält, war die Anforderung der ungeschwärzten Kontoauszüge nicht zulässig. § 25 h Kreditwesengesetz (KWG) rechtfertigt eine derartige Einsichtnahme nicht. Hierfür steht Finanzunternehmen ein unmittelbarer Austausch von Informationen zu einzelnen Vorgängen gem. § 47 Abs. 5 GWG zur Verfügung. Eine Umgehung der dort geregelten Voraussetzungen für einen Informationsaustausch durch Anforderung von Kontoauszügen bei betroffenen Personen ist nicht zulässig.

Zwei weitere Vorgänge betrafen die Schwärzung von Gesundheitsdaten. In Kontoauszügen zu einem bei einem anderen Kreditinstitut geführten Konto, die von einem Kreditinstitut zur Bonitätsprüfung bei der Kreditvergabe angefordert wurden, waren solche Gesundheitsdaten aufgrund der Begleichung von Arztrechnungen enthalten. Da diese Informationen weder für die Kreditvergabe relevant waren, noch für deren Verarbeitung eine Rechtsgrundlage erkennbar war, durften diese Daten auf den Kontoauszügen geschwärzt werden. Auch in einem Rentenbescheid, der aufgrund der Gewährung einer Erwerbsminderungsrente gewährt worden war, durften die Angaben zum Grund der Rentengewährung geschwärzt werden. Auch hier sind die Gesundheitsdaten für die Beurteilung der Bonität nicht erforderlich.

Darüber hinaus gilt für Gesundheitsdaten das grundsätzliche Verbot der Verarbeitung gem. Art. 9 Abs. 1 DS-GVO, sofern nicht ein Ausnahmetatbestand nach Art. 9 Abs. 2 DS-GVO vorliegt. In beiden Fällen war ein solcher Ausnahmetatbestand nicht erkennbar.

11.4
Datenerhebung auf dem Werksgelände eines Unternehmens

Das Auslesen von Daten des Personalausweises mittels eines optischen Lesegerätes bei einer Zutrittskontrolle ist lediglich mittels Einwilligung zulässig. Erteilen betroffene Personen ihre Einwilligung nicht, können die Daten manuell erhoben werden.

Auf dem Werksgelände eines Unternehmens wird bei dem Einlass festgestellt und dokumentiert, welche Personen wann und zu welchem Zweck das Werksgelände betreten und anschließend wieder verlassen. Dazu werden personenbezogene Daten der Besucher und Lieferanten verarbeitet.

Im Rahmen der Anmeldung werden an zwei Eingängen des Werksgeländes optische Scanner eingesetzt, in welche die Personalausweise oder andere Ausweisdokumente der Besucher eingelegt werden. Diese Scanner erfassen personenbezogene Daten der Besucher (Name, Vorname, Ausweisnummer und Gültigkeit des Dokumentes sowie die Unterschrift, mit welcher der

Besucher oder Lieferant die durchgeführte Sicherheitsbelehrung bestätigt). Dies diene der Vermeidung von manuellen Übertragungsfehlern sowie der Verkürzung der Anmeldezeiten. Sodann werden von dem Sicherheitspersonal die Ausweisart (z. B. Personalausweis), das Unternehmen, für das der Besucher tätig ist, der Besuchsempfänger, das Datum und die Uhrzeit des Besuchsbeginns sowie des Besuchsendes händisch ergänzt. Die derart erhobenen Daten werden für die Dauer von zwölf Monaten gespeichert.

Fraglich ist die Rechtsgrundlage der Datenerhebung. Das betreffende Unternehmen führte zum einen Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 4 Nr. 1 lit. c und Nr. 4 Störfall-Verordnung – 12. BImSchV (BGBl. I 2017 S. 483) an.

Art. 6 DS-GVO

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

(…)

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

(…)

§ 4 Störfall-Verordnung – 12. BImSchV

Der Betreiber hat zur Erfüllung der sich aus § 3 Absatz 1 ergebenden Pflicht insbesondere

1. Maßnahmen zu treffen, damit Brände und Explosionen

a) innerhalb des Betriebsbereichs vermieden werden,

b) nicht in einer die Sicherheit beeinträchtigenden Weise von einer Anlage auf andere Anlagen des Betriebsbereichs einwirken können und

c) nicht in einer die Sicherheit des Betriebsbereichs beeinträchtigenden Weise von außen auf ihn einwirken können,

1a. Maßnahmen zu treffen, damit Freisetzungen gefährlicher Stoffe in Luft, Wasser oder Boden vermieden werden,

2. den Betriebsbereich mit ausreichenden Warn-, Alarm- und Sicherheitseinrichtungen auszurüsten,

3. die Anlagen des Betriebsbereichs mit zuverlässigen Messeinrichtungen und Steuer- oder Regeleinrichtungen auszustatten, die, soweit dies sicherheitstechnisch geboten ist, jeweils mehrfach vorhanden, verschiedenartig und voneinander unabhängig sind,

4. die sicherheitsrelevanten Teile des Betriebsbereichs vor Eingriffen Unbefugter zu schützen.

§ 3 Störfall-Verordnung – 12. BImSchV

(1) Der Betreiber hat die nach Art und Ausmaß der möglichen Gefahren erforderlichen Vorkehrungen zu treffen, um Störfälle zu verhindern; Verpflichtungen nach anderen als immissionsschutzrechtlichen Vorschriften bleiben unberührt.

(…)

Das Unternehmen müsse aufgrund seiner Betreiberpflichten für die zuständigen Behörden kontrollieren und dokumentieren, wer weshalb Zugang zum Werksgelände erhalte. Das Besuchermanagement diene ferner dem Datenschutz, da es den Zutritt Unbefugter auf das Werksgelände verhindere, und sei somit ein wichtiger Bestandteil der datenschutzrechtlichen Zugangskontrolle.

Zum anderen wurde als Rechtsgrundlage Art. 6 Abs. 1 lit. f DS-GVO angeführt.

Art. 6 DS-GVO

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

(…)

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.

(…)

Das Unternehmen habe ein berechtigtes Interesse daran, den Zutritt zu seinen Standorten insbesondere zum Schutz des Eigentums nur dazu befugten Personen zu gestatten und das Hausrecht entsprechend auszuüben. Überwiegende schützenswerte Interessen der betroffenen Personen stünden nicht entgegen.

Das Besuchermanagement wurde mit Vertretern des betreffenden Unternehmens ausführlich in einem persönlichen Gespräch in meinem Hause erörtert.

Das Auslesen der Daten des Personalausweises (Vorname, Name, Ausweisnummer und Gültigkeit) mittels eines optischen Lesegerätes aufgrund von Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 4 Nr. 1 lit. c und Nr. 4 Störfall-Verordnung – 12. BImSchV bzw. Art. 6 Abs. 1 lit. f DS-GVO erachte ich als datenschutzrechtlich unzulässig. § 4 Nr. 1 lit. c und Nr. 4 Störfall-Verordnung – 12. BImSchV legitimiert bereits tatbestandlich eine derartige Datenerhebung nicht. Auch

ist die Datenerhebung zum Schutz des Eigentums als berechtigtes Interesse nicht erforderlich. Zudem stehen überwiegende Interessen der betroffenen Personen entgegen. Eine solche Datenerhebung ist lediglich mittels Einwilligung der betroffenen Person möglich. Dies macht überdies § 20 Abs. 2 S. 3 des Personalausweisgesetzes (PAuswG) deutlich.

§ 20 PAuswG

(2) (…) 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.

(…)

Das manuelle Eintragen der Daten per Hand dagegen erachte ich auch ohne Einwilligung für zulässig. Der Prozess zur Erfassung der Daten wurde nach meinen Maßgaben dahingehend angepasst, dass der Einsatz des optischen Scanners nur aufgrund einer Einwilligung stattfindet. Erteilt der Betroffene seine Einwilligung nicht, können die Daten manuell eingetragen werden. Entsprechende Datenschutzhinweise können im Empfangsbereich eingesehen werden. Diese weisen darauf hin, dass der Einsatz des optischen Lesegerätes auf freiwilliger Basis erfolgt.

Zudem habe ich eine weitere Optimierung des Sicherheitsniveaus hinsichtlich der sicheren Aufbewahrung der erhobenen Daten angeraten.

11.5
Lohn- und Gehaltsabrechnung durch Steuerberater

Die Vornahme der Lohn- und Gehaltsabrechnung durch Steuerberater ist nicht als Auftragsverarbeitung zu qualifizieren. Ein entsprechender Vertrag zur Auftragsverarbeitung i. S. d. Art. 28 DS-GVO ist nicht abzuschließen.

Bereits nach bisheriger Rechtslage war unstreitig, dass die klassische steuerberatende Tätigkeit nicht als Auftragsverarbeitung i. S. d. Art. 28 DS-GVO zu qualifizieren ist. Diese Tätigkeit erfolgt in eigener Verantwortung und mit eigenständigem Entscheidungsspielraum. Sehr kontrovers wurde dagegen die Einordnung der Lohn- und Gehaltsabrechnung durch Steuerberater diskutiert. Da Steuerberater, die diese Tätigkeit für Arbeitgeber vornehmen, Mitarbeiterdaten nach fest vorgegebenen Regeln und ohne eigenen Entscheidungsspielraum verarbeiten, habe ich bislang eine Auftragsverarbeitung i. S. d. Art. 28 DS-GVO angenommen. Entsprechend war bei gemischten Leistungsangeboten, d. h. der Vornahme sowohl der klassischen Steuerberatung als

auch der Lohn- und Gehaltsabrechnung durch Steuerberater, jede Leistung separat zu beurteilen. Dann war bzgl. der Lohn- und Gehaltsabrechnung ein Auftragsverarbeitungsvertrag abzuschließen.

Art. 28 DS-GVO

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(…)

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. (…)

(…)

Infolge einer Gesetzesänderung ist diese Auffassung zu revidieren. Gemäß § 11 Abs. 2 des Steuerberatungsgesetzes (StBerG, BGBl. I S. 2451) erfolgt die Verarbeitung personenbezogener Daten durch Steuerberater sowie die weiteren in § 3 StBerG genannten Personen und Gesellschaften (etwa Wirtschaftsprüfer und Steuerberatungsgesellschaften) unter Beachtung der geltenden Berufspflichten weisungsfrei. Diese sind bei der Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO. Die Regelung greift ausweislich der Gesetzesbegründung (BT-Drs. 19/14909 S. 59) für sämtliche Tätigkeiten des Steuerberaters; die Art der Tätigkeit ist daher nicht maßgeblich.

§ 11 StBerG

(…)

(2) Die Verarbeitung personenbezogener Daten durch Personen und Gesellschaften nach § 3 erfolgt unter Beachtung der für sie geltenden Berufspflichten weisungsfrei. Die Personen und Gesellschaften nach § 3 sind bei Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche gemäß Artikel 4 Nummer 7 der Datenschutz-Grundverordnung (EU) 2016/679. Besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 dürfen gemäß Artikel 9 Absatz 2 Buchstabe g der Datenschutz-Grundverordnung (EU) 2016/679 in diesem Rahmen verarbeitet werden.

§ 3 StBerG

Zur geschäftsmäßigen Hilfeleistung in Steuersachen sind befugt:

1. *Steuerberater, Steuerbevollmächtigte, Rechtsanwälte, niedergelassene europäische Rechtsanwälte, Wirtschaftsprüfer und vereidigte Buchprüfer,*
2. *Partnerschaftsgesellschaften, deren Partner ausschließlich die in Nummer 1 genannten Personen sind,*
3. *Steuerberatungsgesellschaften, Rechtsanwaltsgesellschaften, Wirtschaftsprüfungsgesellschaften und Buchprüfungsgesellschaften.*
4. *(weggefallen)*

Damit ist die Vornahme der Lohn- und Gehaltsabrechnung durch Steuerberater nun nicht mehr als Auftragsverarbeitung zu qualifizieren. Ein entsprechender Vertrag zur Auftragsverarbeitung i. S. d. Art. 28 DS-GVO zwischen Auftraggeber und Steuerberater ist nicht abzuschließen.

Die Verarbeitung von Gesundheitsdaten und weiteren „sensiblen" Daten i. S. d. Art. 9 Abs. 1 DS-GVO i. R. d. Tätigkeit von Steuerberatern stützt sich auf Art. 9 Abs. 2 lit. g DS-GVO i. V. m. § 11 Abs. 2 S. 3 StBerG.

Art. 9 DS-GVO

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

(2) Absatz 1 gilt nicht in folgenden Fällen:

(…)

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

(…)

Abschließend ist darauf hinzuweisen, dass im Falle der Übertragung der Lohn- und Gehaltsabrechnung an andere, nicht steuerberatende Dienstleister weiterhin ein Auftragsverarbeitungsvertrag abzuschließen ist.

11.6
Erhebung von Gäste-/Kundendaten während der Corona-Pandemie

Die Erhebung von Gästedaten durch Gaststätten sowie von Kundendaten durch Friseurbetriebe im Zuge der Corona-Pandemie hat verschiedene datenschutzrechtliche Fragestellungen aufgeworfen. Diese führten zu einigen Rechtsunsicherheiten und einer hohen Anzahl an Eingaben bei meiner Behörde.

Nach dem Ende der Corona-bedingten Schließungen durften Gaststätten und andere Gastronomiebetriebe ab Mitte Mai 2020 wieder Speisen und Getränke zum Vor-Ort-Verzehr anbieten. Voraussetzung dafür war jedoch, dass neben der Wahrung der Abstands- und Hygieneregeln auch die Daten der Gäste erfasst werden. Eine entsprechende Regelung findet sich in § 4 Abs. 2 Nr. 3 der Corona-Kontakt- und Betriebsbeschränkungsverordnung (CoKoBeV, Gültigkeit ab 15.05.2020, GVBl. S. 309). Diese stellt eine Rechtsgrundlage i. S. d. Art. 6 Abs. 1 lit. c Abs. 3 DS-GVO dar. Die Vorschrift wurde in späteren Fassungen der CoKoBeV geringfügig modifiziert, inhaltliche Änderungen ergaben sich daraus jedoch nicht.

§ 4 CoKoBeV

(…)

(2) Ab dem 15. Mai 2020 dürfen die in Abs. 1 genannten Betriebe Speisen und Getränke auch zum Verzehr vor Ort anbieten, wenn sichergestellt ist, dass

(…)

3. Name, Anschrift und Telefonnummer der Gäste zur Ermöglichung der Nachverfolgung von Infektionen von der Betriebsinhaberin oder dem Betriebsinhaber erfasst werden; diese haben die Daten für die Dauer eines Monats ab Beginn des Besuchs geschützt vor Einsichtnahme durch Dritte für die zuständigen Behörden vorzuhalten und auf Anforderung an diese zu übermitteln sowie unverzüglich nach Ablauf der Frist zu löschen oder zu vernichten; die Bestimmungen der Art. 13, 15, 18 und 20 der Datenschutz-Grundverordnung zur Informationspflicht und zum Recht auf Auskunft zu personenbezogenen Daten finden keine Anwendung,

(…)

Art. 6 DS-GVO

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

(…)

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

(…)

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(…)

Bereits kurz nach Inkrafttreten der CoKoBeV kam es zu einer hohen Anzahl an Beschwerden bei meiner Behörde. Oftmals wurde eine Datenerhebung für den bloßen Besuch eines Restaurants oder eines Cafés als unverhältnismäßig erachtet. Einige Petenten fürchteten auch das Erstellen etwaiger Persönlichkeitsprofile, da mittels der Gästelisten nachvollziehbar sei, wann sie sich an welchen Orten aufgehalten hätten. In der Folgezeit war das offene Führen der Gästelisten häufiger Beschwerdegegenstand. Manche Gastwirte legten Listen für sämtliche Gäste aus, so dass dritte Personen die Daten anderer Gäste einsehen konnten. Einige Beschwerden richteten sich gegen die Erhebung von nicht zulässigen Daten, etwa von E-Mail-Adressen. Ferner gab es mehrere Eingaben, welche die missbräuchliche Verwendung der erhobenen Gästedaten bemängelten. Diese seien etwa für Werbemaßnahmen oder sonstige Anrufe zweckentfremdet worden. In wenigen Einzelfällen waren diese Beschwerden auch begründet. Auf meinen jeweiligen Hinweis haben die Gaststätten ihr Fehlverhalten eingesehen und sich zukünftig rechtskonform verhalten.

Bei vielen Betreibern war eine Unsicherheit im Umgang mit den datenschutzrechtlichen Anforderungen erkennbar. Dies konnte ich gut nachvollziehen,

da diese sich – in einer ohnehin sehr belastenden Situation – neben den diversen weiteren pandemiebedingten Auflagen hinsichtlich Abstands- und Hygieneregeln auch mit für sie ungewohnten Regelungen des Datenschutzes konfrontiert sahen.

Zur Unterstützung der Gastwirte habe ich bereits kurz nach Inkrafttreten der CoKoBeV im Mai 2020 auf meiner Webseite eine Handlungshilfe zum Umgang mit den Gästedaten veröffentlicht. Die relevanten Maßgaben sollen nachfolgend noch einmal zusammengefasst werden.

Von den Gästen dürfen lediglich die in § 4 Abs. 2 Nr. 3 CoKoBeV enthaltenen Daten und damit nur Name, Anschrift und Telefonnummer erfasst werden. Die Erhebung anderer Daten, insbesondere einer E-Mail-Adresse sowie einer Unterschrift des Gastes, ist unzulässig. Offenkundig falsche Angaben, etwa Pseudonyme oder „Spaßnamen", erfüllen nicht die Anforderungen der CoKoBeV. Da gleichwohl des Öfteren falsche Angaben gemacht worden sind, wurde in einer späteren Fassung der CoKoBeV (Gültigkeit ab 19.10.2020, GVBl. S. 717) zudem eine Regelung eingefügt, nach welcher die Gäste verpflichtet sind, die Daten vollständig und wahrheitsgemäß anzugeben und sie auf Verlangen ihren Personalausweis, Pass, Passersatz oder Ausweisersatz zur Überprüfung ihrer Angaben vorzulegen haben.

Eine bestimmte Form der Datenerhebung ist nicht vorgesehen. Die Gästedaten dürfen jedoch nicht öffentlich zugänglich und für andere Personen einsehbar sein. Die Daten können etwa vom Personal erfasst werden oder den Gästen können einzelne Blätter zum Ausfüllen vorgelegt werden. Auch eine elektronische Datenerfassung (etwa mittels eines QR-Codes oder einer App) ist möglich.

Die Betreiber sind zwar von der Informationspflicht über die Datenerhebung nach Art. 13 DS-GVO befreit. Gleichwohl empfiehlt sich, bereits bei der Erhebung der Daten zu kommunizieren (etwa mittels eines gut sichtbaren Hinweises im Lokal sowie auf den Erfassungsbögen), dass die Datenerhebung zum Zweck der Nachverfolgung von Infektionsketten auf Grundlage von Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 4 Abs. 1 S. 1 Nr. 2 lit. b CoKoBeV erfolgt und dass die Bestimmungen der Art. 13, 15, 18 und 20 DS-GVO keine Anwendung finden. Empfehlenswert ist etwa folgender Passus: *„Die Datenerhebung erfolgt zum Zweck der Nachverfolgung von Infektionsketten auf Grundlage von Art. 6 Abs. 1 lit. c DS-GVO i. V. m. § 4 Abs. 1 S. 1 Nr. 2 lit. b der Corona-Kontakt-und Betriebsbeschränkungsverordnung (CoKoBeV). Die Bestimmungen der Art. 13, 15, 18 und 20 DS-GVO finden keine Anwendung."*

Nach der Erfassung sind die Gästedaten geschützt vor Einsichtnahme durch Dritte aufzubewahren, etwa in einem verschlossenen Schrank bzw. Tresor, zu dem möglichst wenige Personen Zugang haben sollten.

Da die Gästedaten für die Dauer eines Monats ab Beginn des Besuches vorzuhalten sind, empfiehlt es sich, die Gästedaten taggenau zu führen und diese einen Monat nach dem Besuch des Gastes zu vernichten. Falls die zuständige Behörde die Herausgabe der Gästedaten bereits vor Ablauf des Monats angefordert hat, sind die Gästedaten an diese herauszugeben und danach unverzüglich zu vernichten.

Die Gästedaten sind regelmäßig an die Gesundheitsämter, in Eilfällen an die örtlichen Ordnungsbehörden, herauszugeben, vgl. § 7 CoKoBeV. Die Daten dürfen an keine anderen Stellen übermittelt werden. Diese sind auch nicht für andere Zwecke, etwa für Telefonanrufe infolge einer unbezahlten Rechnung eines Gastes, zu verwenden.

§ 7 CoKoBeV

Für den Vollzug dieser Verordnung sind abweichend von § 5 Abs. 1 des Hessischen Gesetzes über den öffentlichen Gesundheitsdienst vom 28. September 2007 (GVBl. I S. 659), zuletzt geändert durch Gesetz vom 3. Mai 2018 (GVBl. S. 82), neben den Gesundheitsämtern die örtlichen Ordnungsbehörden zuständig, wenn die Gesundheitsämter nicht rechtzeitig erreicht oder tätig werden können, um eine bestehende Gefahrensituation abwenden zu können.

Die Löschung oder Vernichtung der Gästedaten muss sicher und datenschutzkonform erfolgen. Auf Papier erfasste Daten sind etwa in einem Aktenvernichter bzw. Papierschredder zu vernichten. Da sicherzustellen ist, dass dritte Personen keine Kenntnis von den Gästedaten erlangen, genügt ein händisches Zerreißen oder das bloße Wegwerfen der Zettel in den Papiermüll nicht.

Zwecks Kontrolle, ob den datenschutzrechtlichen Anforderungen auch in der Praxis genügt wird, habe ich einen Fragebogen an 100 über ganz Hessen verteilte Gastronomiebetriebe versendet. Dabei zeigte sich, dass die Betriebe ganz überwiegend den datenschutzrechtlichen Anforderungen gerecht werden. Die Erhebung erfolgt fast durchgehend in papierner Form auf Einzelblättern. Häufig wird das Musterformular des DEHOGA Hessen e. V. verwendet. Die sichere Aufbewahrung und Vernichtung der Daten waren den Teilnehmern ganz überwiegend bewusst. Unsicherheiten zeigten sich jedoch öfters bzgl. der korrekten Aufbewahrungsfrist von einem Monat. Eine Herausgabe der Daten wurde ausnahmslos verneint.

Des Weiteren habe ich in Zusammenarbeit mit dem DEHOGA Hessen e. V. entsprechende Informationen zur Erhebung der Gästedaten an Gaststätten verteilt.

Mit diesen Maßnahmen konnte ich eine deutliche Verbesserung hinsichtlich der Einhaltung der datenschutzrechtlichen Maßgaben erreichen. Dies zeigte sich auch darin, dass das Beschwerdeaufkommen bei meiner Behörde signifikant rückläufig war. Viele Gastwirte bedankten sich für die bereitgestellten Informationen, mit denen sie den datenschutzrechtlichen Anforderungen in der Praxis besser begegnen konnten.

Neben der Erhebung der Gästedaten in Gaststätten beschäftigte mich auch die Datenerfassung der Kunden von Friseurbetrieben. Anders als für Gaststätten gab es für Friseurbetriebe in der CoKoBeV zunächst keine gesetzliche Grundlage zur Erhebung von Kundendaten. Gleichwohl veröffentlichte die Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege (BGW) einen Leitfaden auch zu der Erhebung von Kundendaten, der jedoch einige datenschutzrechtliche Fragen, insbesondere hinsichtlich der Rechtsgrundlage der Datenerhebung, aufgeworfen hat.

Um auch die Friseurbetriebe bei der Erfüllung der datenschutzrechtlichen Anforderungen zu unterstützen, veröffentlichte ich Mitte Mai 2020 eine entsprechende Handlungshilfe auf meiner Webseite. Meine Empfehlungen orientierten sich größtenteils an den Regelungen der Datenerfassung durch Gaststätten nach der CoKoBeV. Mangels ausdrücklicher Rechtsgrundlage erachtete ich die Erfassung der Kundendaten durch Friseurbetriebe aufgrund von Art. 6 Abs. 1 lit. f DS-GVO für zulässig.

Art. 6 DS-GVO

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

(…)

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.

(…)

Auch bei den Friseurbetrieben ist insbesondere darauf zu achten, dass die Kundendaten für dritte Personen nicht einsehbar sind und die Daten nach Ablauf von einem Monat datenschutzkonform vernichtet werden. Im Unterschied zu den Gaststätten waren Friseurbetriebe weder von der Informationspflicht nach Art. 13 DS-GVO befreit, noch bestanden Einschränkungen bei der Erfüllung der Betroffenenrechte nach Art. 15 ff. DS-GVO.

In einer späteren Fassung der CoKoBeV (Gültigkeit ab 19.10.2020, GVBl. S. 717) wurde sodann auch für Friseurbetriebe eine ausdrückliche gesetzliche Regelung zur Datenerhebung geschaffen, die sich an der bereits bestehenden Regelung für Gaststätten orientiert, vgl. § 6 Abs. 3 CoKoBeV. Fortan ist die Datenerhebung seitens der Friseurbetriebe aufgrund von Art. 6 Abs. 1 lit. c Abs. 3 DS-GVO i. V. m. § 6 Abs. 3 CoKoBeV legitimiert.

§ 6 CoKoBeV

(…)

(3) Die Betreiber von Betrieben und Einrichtungen nach Abs. 2 Satz 1 haben sicherzustellen, dass Name, Anschrift und Telefonnummer der Kundinnen und Kunden ausschließlich zur Ermöglichung der Kontaktnachverfolgung von Infektionen erfasst werden; sie haben die Daten für die Dauer eines Monats ab Beginn des Besuchs geschützt vor Einsichtnahme durch Dritte für die zuständigen Behörden vorzuhalten und auf Anforderung an diese zu übermitteln sowie unverzüglich nach Ablauf der Frist sicher und datenschutzkonform zu löschen oder zu vernichten; die Bestimmungen der Art. 13, 15, 18 und 20 der Datenschutz-Grundverordnung finden keine Anwendung; die Kundinnen und Kunden sind über diese Beschränkung zu informieren.

Wenngleich das Beschwerdeaufkommen hinsichtlich der Datenerfassung bei Friseurbetrieben geringer als bei Gaststätten ausfiel, erreichten mich auch diesbezüglich einige Eingaben, insbesondere zu dem offenen Führen von Kundenlisten und der missbräuchlichen Verwendung von Kundendaten. Auch hier war jedoch eine stetige Abnahme der Beschwerden zu verzeichnen, so dass die datenschutzrechtlichen Anforderungen seitens der Friseurbetriebe in der Praxis zunehmend eingehalten worden sind.

11.7
Sichere Aktenvernichtung bei Rechtsanwaltskanzleien

Berufsgeheimnisträger, wie Rechtsanwältinnen und Rechtsanwälte, treffen besondere Sorgfaltspflichten bei der datenschutzgerechten Vernichtung von Papierdokumenten und Arbeitsunterlagen, die personenbezogene Daten Dritter enthalten.

Ein Beschwerdeführer wandte sich mit dem Hinweis an den HBDI, er habe vollständig lesbare Papierdokumente einer Rechtsanwaltskanzlei im Papiermüllcontainer eines Mehrparteienhauses vorgefunden. Der Beschwerdeführer übersandte zum Beweis Fotos von zahlreichen Dokumenten. Darunter befand sich vertrauliche Korrespondenz mit Mandanten, Kontoauszüge, Rechnungen und weitere Dokumente mit personenbezogenen Daten. In ei-

nem anderen Fall wurde dem HBDI gemeldet, dass Papierdokumente einer Rechtsanwaltskanzlei mit vertraulichen personenbezogenen Daten über eine Straße verteilt auf dem Boden lagen. Die bezeichneten Unterlagen bergen in falschen Händen ein großes Missbrauchspotenzial.

Da es sich bei den Verantwortlichen um Berufsgeheimnisträger handelte, die regelmäßig mit einer Vielzahl vertraulicher personenbezogener Daten umgehen, wogen die Sachverhalte schwerer, als wenn es sich um Verantwortliche ohne die Berufsgeheimnisträgereigenschaft gehandelt hätte. Eine unberechtigte Kenntnisnahme Dritter hat zumindest im ersten Fall stattgefunden und könnte in der zweiten Fallkonstellation jederzeit stattfinden.

Vor allem besteht grundsätzlich das Risiko, dass Papierdokumente auf dem Entsorgungsweg verloren gehen. Auch wenn es sich hier um analog verarbeitete personenbezogene Daten handelt, ergibt sich aus den zurückgelegten Fahrtwegen der Entsorgungsbetriebe eine erhebliche Streubreite.

In jedem Fall gilt es zu beachten, dass Papierdokumente mit personenbezogenen Daten, die nicht aus dem privaten Bereich stammen, mittels eines Aktenvernichters oder qualifizierten Entsorgungsdienstes zu vernichten sind. Es handelt sich hierbei um technische und organisatorische Maßnahmen i. S. v. Art. 32 DS-GVO, welche die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten.

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;

(…)

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

(…)

Hierfür ist nach dem Stand der Technik bei besonders sensiblen Daten mindestens die Sicherheitsstufe P-4 gemäß der Norm DIN/ISO 66399-2 zu erfüllen. Diese Sicherheitsstufe schreibt eine Zerkleinerung mittels des sogenannten Partikelschnitts (cross-cut) vor. Ähnliche Vorkommnisse sind

bereits in meinen vorangegangenen Tätigkeitsberichten thematisiert worden (vgl. 48. Tätigkeitsbericht, S. 72 ff.). Auch in einer zunehmend digitalisierten Welt sollte man den sachgerechten Umgang mit und die sichere Vernichtung von Papierdokumenten nicht aus den Augen verlieren.

Ich habe nach Abschluss der Sachverhaltsermittlung die erforderlichen aufsichtsbehördlichen Maßnahmen ergriffen.

12. Auskunfteien, Inkassounternehmen

12.1
Scoringverfahren der SCHUFA Holding AG

Zur Verbesserung der erzielten Scoringergebnisse hat die SCHUFA Holding AG (SCHUFA) ihr Scoringverfahren modifiziert und das modifizierte Scoringverfahren erläutert.

Das Scoringverfahren der SCHUFA unterliegt als Geschäftsgeheimnis einem besonderen Schutz und muss von der SCHUFA auch im Zuge der Erfüllung von Auskunftspflichten nach Art. 15 DS-GVO nicht im Einzelnen offengelegt werden (BGH, Urteil vom 28.01.2014, Az. VI ZR 156/13, *https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=d16415a2f250c4a65e28a44a9ee34a17&nr=66910&pos=0&anz=1*). Mir gegenüber ist die SCHUFA aber dennoch zur Offenlegung ihrer Scoringverfahren im Rahmen meiner Aufsichtstätigkeit verpflichtet. Dieser Verpflichtung ist die SCHUFA nach Änderungen im Scoringverfahren unaufgefordert nachgekommen.

Hierbei hat die SCHUFA sowohl das geänderte Verfahren detailliert erläutert, als auch die Gründe für die Änderungen im Verfahren dargestellt. Zusätzlich hat die SCHUFA ein wissenschaftliches Gutachten vorgelegt, in dem das Verfahren analysiert und bewertet wird.

Aus der Darstellung der SCHUFA und dem Inhalt des Gutachtens ergab sich, dass die verwendeten Verfahren den Anforderungen an Scoringverfahren gemäß § 31 Abs. 1 Nr. 2 BDSG entsprechen. Bei den verwendeten Verfahren handelt es sich sowohl nach dem Inhalt des vorgelegten Gutachtens als auch nach meiner Erkenntnis um wissenschaftlich anerkannte mathematisch-statistische Verfahren. Die benutzten Daten sind zur Berechnung der Wahrscheinlichkeit für die Rückzahlung eines gewährten Kredites erheblich. Weder aus der Darstellung der SCHUFA noch aus dem Inhalt des Gutachtens ergaben sich daran Zweifel.

Mit der Änderung der bisherigen Verfahren werden die von der SCHUFA verwendeten Scoringverfahren an neuere wissenschaftliche Entwicklungen zur Scorewertberechnung angepasst. Mit der Verfahrensänderung sind Verbesserungen der Trennschärfe und damit der Scorewerte zu erwarten. Die Änderung der Verfahren wird daher von mir positiv beurteilt.

12.2
Die Umsetzung der Informationspflicht nach Art. 14 DS-GVO im Bereich der Auskunfteien

Im Falle einer Dritterhebung von personenbezogenen Daten durch Auskunfteien erfolgt hierzu nach Art. 14 DS-GVO eine proaktive und für die betroffene Person anlasslose Information durch Auskunfteien gegenüber der betroffenen Person.

Ein erhebliches Beschwerdeaufkommen resultiert aus den durch Auskunfteien an Betroffene versandten Schreiben vor dem Hintergrund der Informationspflicht nach Art. 14 DS-GVO. Werden personenbezogene Daten bei einem Dritten und nicht unmittelbar bei der betroffenen Person selbst erhoben (sog. „Dritterhebung"), so ist der Verantwortliche dazu verpflichtet, der betroffenen Person die unter Art. 14 DS-GVO aufgeführten Informationen mitzuteilen. Hierunter fallen u. a. Informationen zu dem Namen und den Kontaktdaten des Verantwortlichen, den Kontaktdaten des Datenschutzbeauftragten, den Zwecken und der Rechtsgrundlage der Datenverarbeitung sowie Ausführungen zu den Betroffenenrechten. Ferner ist zu berücksichtigen, dass Auskunfteien Informationen grundsätzlich nicht nur bei Dritten, sondern auch durch Dritte erheben können.

Die durch Auskunfteien mittels Versendung von Informationsschreiben erfüllte gesetzliche Verpflichtung nach Art. 14 DS-GVO führt jedoch bei den Empfängern regelmäßig zu Irritationen, da die Informationen oft falsch interpretiert werden. So hatte eine Vielzahl von Empfängern bislang noch keine wissentlich wahrgenommenen Berührungspunkte mit Auskunfteien und geht irrtümlich von einer missbräuchlich erfolgten Erhebung und Verarbeitung der personenbezogenen Daten aus.

Bei Auskunfteien handelt es sich um private gewerbliche Unternehmen. Sie erheben Informationen über die Identität, die wirtschaftliche Betätigung, die Kreditwürdigkeit, die Zahlungswilligkeit und -fähigkeit von Unternehmen und Privatpersonen. Diese Informationen werden gespeichert und an Dritte übermittelt, wenn diese ein berechtigtes Interesse an einer solchen Information haben. Insbesondere dürfen Auskunfteien verschiedene personenbezogene Daten aufgrund einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO verarbeiten. Zulässig ist u. a. die Verarbeitung von Identifikationsdaten (z. B. Name, Vorname, Adresse, Geburtsdatum und frühere Anschriften). Diese Informationen dienen der korrekten Zuordnung der Daten sowie der Vermeidung von Personenverwechselungen. Darüber hinaus ist die Berechnung von Scorewerten durch Auskunfteien zulässig, sofern die Voraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO i. V. m. § 31 BDSG erfüllt sind. Dabei handelt

es sich um statistisch begründete Prognosewerte bezüglich des zukünftigen Risikos eines Zahlungsausfalles, die beispielsweise als Entscheidungskriterium dafür herangezogen werden können, ob ein Kauf auf Rechnung bei Fernabsatzgeschäften im Internet angeboten wird. Somit ist die Umsetzung der Informationspflicht für die Betroffenen hinsichtlich der Kenntnis über den eigenen Scorewert zunehmend wichtig.

Eine in der behördlichen Aufsichtspraxis oftmals wiederkehrende Sachverhaltskonstellation stellt insbesondere die Adressrecherche durch Auskunfteien im Falle von nicht zustellbaren Schreiben aufgrund eines Umzuges dar. Ergibt sich beispielsweise bei einem Kauf auf Rechnung ein kreditorisches Risiko seitens des Gläubigers, besteht ein berechtigtes Interesse an der Kenntnis der aktuellen Anschrift des Rechnungsadressaten, um etwaige Forderungsansprüche geltend machen zu können. In diesem Fall ermitteln Auskunfteien im Auftrag des Gläubigers die aktuelle Adresse bei Dritten (z. B. Einwohnermeldeämtern) und informieren anschließend die Betroffenen über die Datenerhebung und -verarbeitung nach Art. 14 DS-GVO.

Durch ein Informationsschreiben nach Art. 14 DS-GVO wird die betroffene Person in die Lage versetzt, die im Einzelfall erfolgte Datenverarbeitung nachvollziehen zu können. Grundsätzlich wird ergänzend empfohlen, den Auskunftsanspruch nach Art. 15 DS-GVO geltend zu machen. Demnach sind Auskunfteien dazu verpflichtet, umfassend und kostenfrei über die gespeicherten Daten Auskunft zu erteilen. Sollte eine Prüfung der nach Art. 15 DS-GVO erteilten Auskunft ergeben, dass personenbezogene Daten fehlerhaft im Datenbestand von Auskunfteien geführt werden, bestehen Ansprüche auf Berichtigung, Löschung oder Einschränkung der Verarbeitung entsprechender Daten nach den Art. 16 bis 18 DS-GVO.

Im Ergebnis zielt die durch Art. 14 DS-GVO begründete aktive Informationspflicht für Auskunfteien im Falle von Dritterhebungen auf eine Gewährleistung der Transparenz der Datenverarbeitungsprozesse ab und erleichtert in der Folge zugleich die etwaige Wahrnehmung von Betroffenenrechten.

12.3
Zulässigkeit der Verarbeitung von (Forderungs-)Daten seitens der Inkassounternehmen

Die Verarbeitung personenbezogener Daten vermeintlicher Schuldner/-innen seitens der Inkassounternehmen (nachfolgend: IKU) ist auch in den Fällen von Personenverwechslungen oder auch in Fällen, bei denen sich herausstellt, dass die Forderung seitens des Schuldners bzw. der Schuldnerin bereits vor

Mandatierung des IKU an die Gläubigerin oder auch nach Mandatierung des IKU unmittelbar an das IKU beglichen wurde, zunächst grundsätzlich zulässig.

Häufig erreichen mich Beschwerden betroffener Personen, die auf die unverzügliche und vollumfängliche Löschung ihrer Daten aus dem Datensatz des jeweiligen IKU abzielen.

Die Beschwerden werden damit begründet, dass die betroffene Person nicht Schuldner/-in der geltend gemachten Forderung oder die Forderung im Rahmen des Inkassoverfahrens bereits beglichen sei. Eine Speicherung der entsprechenden Daten seitens der IKU sei deshalb nicht mehr erforderlich und es habe die Löschung zu erfolgen.

In weiteren, jedoch seltenen Fällen wird ausgeführt, der/die Schuldner/-in habe die Forderung bereits vor Mandatierung des IKU an die Gläubigerin bezahlt. Die Datenübermittlung an das IKU sowie die dortige Speicherung der Daten der betroffenen Person seien daher rechtswidrig.

Grundsätzliches zur Zulässigkeit der Datenverarbeitung seitens des IKU

Grundsätzlich ist die Mandatierung eines IKU (gleich einer Anwaltskanzlei) zum Zweck der Realisierung offener Forderungen aufgrund der Privatautonomie zulässig. Hierfür ist die Übermittlung von Daten (Vertrags- bzw. Forderungsdaten sowie Daten des/der Schuldners/-in, insbesondere Namen und Anschrift, der Forderungsgrund, die Höhe und die Fälligkeit der Forderung etc.) seitens der Gläubigerin an das IKU erforderlich und aus datenschutzrechtlicher Sicht nicht zu beanstanden: Die entsprechende Datenverarbeitung erfolgt in diesen Fällen auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO zur Durchsetzung der schuldnerseitigen Erfüllung des Vertrages mit der Gläubigerin sowie auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO zur Wahrung berechtigter Interessen des IKU bzw. der Gläubigerin.

Eine Einwilligung der betroffenen Person zu dieser Datenverarbeitung ist demnach nicht erforderlich. Sofern die betroffene Person gegenüber dem IKU eine etwaig erteilte Einwilligung (präventiv) widerruft, kann ein derartiger Widerruf folglich dahinstehen; dieser ist aus datenschutzrechtlicher Sicht schlicht nicht relevant.

Art. 6 Abs. 1 DS-GVO lautet wie folgt:

Art. 6 DS-GVO

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

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

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

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

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

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

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

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

Ein Recht auf Löschung von Daten gegenüber dem IKU kann sich zu Gunsten der betroffenen Person aus Art. 17 Abs. 1 DS-GVO unter den dort genannten Voraussetzungen ergeben.

Art. 17 DS-GVO lautet wie folgt:

Art. 17 DS-GVO

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

(2) Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er gemäß Absatz 1 zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

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

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information;

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;

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Artikel 9 Absatz 2 Buchstaben h und i sowie Artikel 9 Absatz 3;

d) für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1, soweit das in Absatz 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Datenverarbeitung bei erfolgtem Ausgleich der Forderung gegenüber dem IKU

Im Falle des Ausgleichs des Forderungsbetrages an das IKU und damit dem Abschluss des Inkassoverfahrens scheint zunächst gem. Art. 17 Abs. 1 lit. a DS-GVO zu Gunsten des/der Schuldners/-in ein Recht auf Löschung der entsprechenden Daten zu bestehen. Schließlich sind diese für den Zweck, für den Sie erhoben wurden (Vertragsabwicklung/Rechtsverfolgung/Forderungsmanagement), nun nicht mehr erforderlich: Dieser Zweck ist durch den Forderungsausgleich weggefallen.

Gleichwohl kann die weitere Verarbeitung aus anderen Gründen auch weiterhin zulässig sein. Vorliegend ist die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der das IKU unterliegt. Eine solche rechtliche Verpflichtung des IKU zur weiteren Datenspeicherung ergibt sich insbesondere aus den steuer- und handelsrechtlichen Aufbewahrungs- und Dokumentationspflichten, denen das IKU nach § 147 Abgabenordnung (AO)

sowie § 257 Handelsgesetzbuch (HGB) unterliegt. Danach sind die entsprechende Geschäftskorrespondenz sowie Buchungsbelege etc. jeweils für einen Zeitraum von sechs Jahren bzw. zehn Jahren aufzubewahren. Darüber hinaus sind die Daten für das IKU erforderlich, um die eigene Tätigkeit gegenüber dem Auftraggeber und dem/der Schuldner/-in abzurechnen und ggf. den Nachweis über die Berechtigung der vereinnahmten oder beanspruchten Gebühren zu führen. Weiterhin werden die Daten seitens des IKU benötigt, um Rückfragen der jeweils zuständigen Datenschutzaufsichtsbehörde im Rahmen entsprechender Einzelfallprüfungen beantworten zu können. Nach alledem besteht gem. 17 Abs. 3 lit. b DS-GVO zunächst noch kein Anspruch auf Löschung.

§ 147 AO und § 257 HGB lauten wie folgt:

§ 147 AO (1)

(1) Die folgenden Unterlagen sind geordnet aufzubewahren:

1. *Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,*
2. *die empfangenen Handels- oder Geschäftsbriefe,*
3. *Wiedergaben der abgesandten Handels- oder Geschäftsbriefe,*
4. *Buchungsbelege,*

4a. *Unterlagen nach Artikel 15 Absatz 1 und Artikel 163 des Zollkodex der Union,*

5. *sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.*

(2) Mit Ausnahme der Jahresabschlüsse, der Eröffnungsbilanz und der Unterlagen nach Absatz 1 Nummer 4a, sofern es sich bei letztgenannten Unterlagen um amtliche Urkunden oder handschriftlich zu unterschreibende nicht förmliche Präferenznachweise handelt, können die in Absatz 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, dass die Wiedergabe oder die Daten mit den empfangenen Handels- oder Geschäftsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden, während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich lesbar gemacht und maschinell ausgewertet werden können.

(3) Die in Absatz 1 Nr. 1, 4 und 4a aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren, sofern nicht in anderen Steuergesetzen kürzere Aufbewahrungsfristen zugelassen sind. Kürzere Aufbewahrungsfristen nach außersteuerlichen Gesetzen lassen die in Satz 1 bestimmte Frist unberührt. Bei empfangenen Lieferscheinen, die keine Buchungsbelege nach Absatz 1 Nummer 4 sind, endet die Aufbewahrungsfrist mit dem Erhalt der Rechnung. Für abgesandte Lieferscheine, die keine Buchungsbelege nach Absatz 1 Nummer 4 sind, endet die Aufbewahrungsfrist mit dem Versand der Rechnung. Die Aufbewahrungsfrist läuft jedoch nicht ab, soweit und solange die Unterlagen für Steuern von Bedeutung sind, für welche die Festsetzungsfrist noch nicht abgelaufen ist; § 169 Abs. 2 Satz 2 gilt nicht.

(4) Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Buch gemacht, das Inventar, die Eröffnungsbilanz, der Jahresabschluss oder der Lagebericht aufgestellt, der Handels- oder Geschäftsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist, ferner die Aufzeichnung vorgenommen worden ist oder die sonstigen Unterlagen entstanden sind.

(5) Wer aufzubewahrende Unterlagen in der Form einer Wiedergabe auf einem Bildträger oder auf anderen Datenträgern vorlegt, ist verpflichtet, auf seine Kosten diejenigen Hilfsmittel zur Verfügung zu stellen, die erforderlich sind, um die Unterlagen lesbar zu machen; auf Verlangen der Finanzbehörde hat er auf seine Kosten die Unterlagen unverzüglich ganz oder teilweise auszudrucken oder ohne Hilfsmittel lesbare Reproduktionen beizubringen.

(6) Sind die Unterlagen nach Absatz 1 mit Hilfe eines Datenverarbeitungssystems erstellt worden, hat die Finanzbehörde im Rahmen einer Außenprüfung das Recht, Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Sie kann im Rahmen einer Außenprüfung auch verlangen, dass die Daten nach ihren Vorgaben maschinell ausgewertet oder ihr die gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung gestellt werden. Teilt der Steuerpflichtige der Finanzbehörde mit, dass sich seine Daten nach Absatz 1 bei einem Dritten befinden, so hat der Dritte

1. *der Finanzbehörde Einsicht in die für den Steuerpflichtigen gespeicherten Daten zu gewähren oder*
2. *diese Daten nach den Vorgaben der Finanzbehörde maschinell auszuwerten oder*
3. *ihr die für den Steuerpflichtigen gespeicherten Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Verfügung zu stellen.*

Die Kosten trägt der Steuerpflichtige. In Fällen des Satzes 3 hat der mit der Außenprüfung betraute Amtsträger den in § 3 und § 4 Nummer 1 und 2 des Steuerberatungsgesetzes bezeichneten Personen sein Erscheinen in angemessener Frist anzukündigen. Sofern noch nicht mit einer Außenprüfung begonnen wurde, ist es im Fall eines Wechsels des Datenverarbeitungssystems oder im Fall der Auslagerung von aufzeichnungs- und aufbewahrungspflichtigen Daten aus dem Produktivsystem in ein anderes Datenverarbeitungssystem ausreichend, wenn der Steuerpflichtige nach Ablauf des fünften Kalenderjahres, das auf die Umstellung oder Auslagerung folgt, diese Daten ausschließlich auf einem maschinell lesbaren und maschinell auswertbaren Datenträger vorhält.

§ 257 Handelsgesetzbuch

(1) Jeder Kaufmann ist verpflichtet, die folgenden Unterlagen geordnet aufzubewahren:

1. *Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse nach § 325 Abs. 2a, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,*
2. *die empfangenen Handelsbriefe,*
3. *Wiedergaben der abgesandten Handelsbriefe,*
4. *Belege für Buchungen in den von ihm nach § 238 Abs. 1 zu führenden Büchern (Buchungsbelege).*

(2) Handelsbriefe sind nur Schriftstücke, die ein Handelsgeschäft betreffen.

(3) Mit Ausnahme der Eröffnungsbilanzen und Abschlüsse können die in Absatz 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden, wenn dies den Grundsätzen ordnungsmäßiger Buchführung entspricht und sichergestellt ist, daß die Wiedergabe oder die Daten

1. *mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,*
2. *während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können.*

Sind Unterlagen auf Grund des § 239 Abs. 4 Satz 1 auf Datenträgern hergestellt worden, können statt des Datenträgers die Daten auch ausgedruckt aufbewahrt werden; die ausgedruckten Unterlagen können auch nach Satz 1 aufbewahrt werden.

(4) Die in Absatz 1 Nr. 1 und 4 aufgeführten Unterlagen sind zehn Jahre, die sonstigen in Absatz 1 aufgeführten Unterlagen sechs Jahre aufzubewahren.

(5) Die Aufbewahrungsfrist beginnt mit dem Schluss des Kalenderjahrs, in dem die letzte Eintragung in das Handelsbuch gemacht, das Inventar aufgestellt, die Eröffnungsbilanz oder der Jahresabschluss festgestellt, der Einzelabschluss nach § 325 Abs. 2a oder der Konzernabschluss aufgestellt, der Handelsbrief empfangen oder abgesandt worden oder der Buchungsbeleg entstanden ist.

Vielmehr tritt in diesen Fällen gemäß Art. 17 Abs. 3 lit. b DS-GVO i. V. m. § 35 Abs. 3 BDSG an die Stelle einer Löschung der Daten die Einschränkung der Verarbeitung der entsprechenden Daten der betroffenen Person.

In der Praxis der Fallbearbeitung der IKU werden daher nach Abschluss des jeweiligen Inkassoverfahrens die Daten für eine etwaige (Inkasso-)Bearbeitung entsprechend gesperrt und jeweils nach Ablauf der vorbezeichneten Aufbewahrungsfristen seitens des IKU gelöscht.

§ 35 BDSG lautet:

§ 35 BDSG

(1) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 der Verordnung (EU) 679/2016 ergänzend zu den in Artikel 17 Absatz 3 der Verordnung (EU) 679/2016 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 679/2016. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) Ergänzend zu Artikel 18 Absatz 1 Buchstabe b und c der Verordnung (EU) 679/2016 gilt Absatz 1 Satz 1 und 2 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a und d der Verordnung (EU) 679/2016, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Artikel 17 Absatz 3 Buchstabe b der Verordnung (EU) 679/2016 gilt Absatz 1 entsprechend im Fall des Artikels 17 Absatz 1 Buchstabe a der Verordnung (EU) 679/2016, wenn einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen.

Datenverarbeitung bei erfolgtem Ausgleich der Forderung gegenüber der Gläubigerin

Die vorausgeführten Grundsätze hinsichtlich der Aufbewahrungs- bzw. Speicherverpflichtung seitens der IKU sowie der vorgenannten Löschfristen gelten auch für diejenigen Fälle, bei denen die betroffene Person ihre Verbindlichkeit bereits vor Mandatierung des IKU unmittelbar gegenüber der Gläubigerin zum Ausgleich gebracht hat.

Derartige Fälle basieren in der Regel auf einer zeitlichen „Überschneidung" des Zahlungseingangs bei der Gläubigerin und der Datenübermittlung an das IKU.

Aufgrund der geleisteten Zahlung war die Mandatierung des IKU zwar unnötig: Schließlich hatte der/die vormalige Schuldner/-in seine/ihre vertragliche Verpflichtung bereits erfüllt.

Daher besteht zivilrechtlich in aller Regel auch kein Anspruch auf Zahlung der Kosten einer derartigen Beauftragung durch den Schuldner. Diese treffen vielmehr die Gläubigerin. Diese hat daher grundsätzlich kein Interesse an dieser unnötigen Beauftragung. Gleichwohl kommt eine solche in Einzelfällen vor.

In diesen Fällen schränkt die DS-GVO die Privatautonomie grundsätzlich nicht ein. Eine derart versehentliche Beauftragung ist daher zumindest aus Gründen des Datenschutzes nicht per se rechtswidrig. Die Geltendmachung einer Forderung nach einer Beauftragung ist nur dann möglich, wenn das IKU über die Forderungsdaten verfügt. Diese Datenübermittlung ist daher notwendiger Bestandteil der Mandatierung eines IKU und damit gem. Art. 6 Abs. 1 Satz 1 lit. c DS-GVO zulässig. Daraus folgt jedoch nicht, dass jede Übermittlung aufgrund einer vertraglichen Verpflichtung gem. Art. 6 Abs. 1 Satz 1 lit. c DS-GVO zulässig ist. Wird ein zivilrechtlicher Vertrag lediglich zur Legitimierung einer Datenübermittlung geschlossen oder werden in einen solchen Vertrag zur Legitimierung einer Datenübermittlung entsprechende

Regelungen aufgenommen, kann dieser Vertrag die Datenübermittlung nicht legitimieren.

Auch in diesem Falle ist durch die erfolgte Übernahme des Inkassomandats bei dem IKU ein Geschäftsvorfall entstanden. Dieser Geschäftsvorfall löst für das IKU die oben bereits dargelegten Dokumentations- und Aufbewahrungspflichten aus. Folglich sind seitens des IKU die entsprechenden Dokumente bzw. Daten auch in dieser Fallkonstellation – in den für die Inkassobearbeitung gesperrten Dateien – mit dem eingeschränkten Verarbeitungszweck für Zeiträume von bis zu zehn Jahren aufzubewahren bzw. zu speichern.

Gleichwohl hat der Gläubiger in derartigen Fällen aufgrund seiner Verpflichtungen zur Datenminimierung gem. Art. 5 Abs. 1 lit. c DS-GVO und Richtigkeit gem. Art. 5 Abs. 1 lit. d DS-GVO vor einer Mandatierung eines IKU sorgfältig zu prüfen, ob eine Mandatierung erforderlich ist. Wurde eine solche Prüfung nicht vorgenommen oder keine ausreichenden Verfahren zur Verhinderung unnötiger Mandatierungen implementiert, kann dennoch ein Verstoß gegen die DS-GVO aufseiten der Gläubigerin vorliegen.

Datenverarbeitung im Falle einer Personenverwechslung

Auch im Falle einer Personenverwechslung stellt sich die Rechtslage wie oben beschrieben dar. Durch die Geltendmachung der Forderung seitens des IKU – auch gegenüber dem/der unzutreffenden Schuldner/-in bzw. der verwechselten Person – ist seitens des IKU ebenfalls ein Geschäftsvorfall entstanden, der die entsprechenden Dokumentations- und Aufbewahrungspflichten begründet. Eine vorzeitige Löschung der Daten der verwechselten Person kommt demnach auch in diesen Fällen nicht in Betracht.

Ursache für eine solche Personenverwechslung ist oftmals die Tatsache, dass der/die tatsächliche Schuldner/-in unbekannt verzogen ist. Dies führt zu Postrückläufern hinsichtlich der Rechnungen bzw. Mahnschreiben, was wiederum seitens der IKU eine Adressrecherche bei einer Wirtschaftsauskunftei oder einem Adressdienstleister auslöst. Hierbei kann es im negativen Fall (beispielsweise bei namensgleichen Personen, die in derselben Stadt wohn(t)en etc.) seitens der Wirtschaftsauskunftei oder dem Adressdienstleister irrtümlich zu einer unzutreffenden Zuordnung des angefragten Datensatzes zu dem dort gespeicherten Datensatz oder einer zutreffenden Zuordnung zu einem unzutreffenden Datensatz – und somit zu der Personenverwechslung – kommen.

Mit den daraufhin seitens der Wirtschaftsauskunftei oder dem Adressdienstleister an das IKU übermittelten, vermeintlich neuen Adressdaten des/der vermeintlichen Schuldners/-in wird nun im Rahmen des Forderungsmanage-

ments die verwechselte Person seitens des IKU angeschrieben. Dies ist für die Betroffenen naturgemäß in jedweder Hinsicht äußerst unerfreulich.

In einem solchen Fall ist es für Betroffene – zur Vermeidung weiterer Inkassomaßnahmen und damit verbundener Unannehmlichkeiten – empfehlenswert, unverzüglich Kontakt mit dem IKU aufzunehmen und dieses auf die bestehende Personenverwechslung hinzuweisen. Hierdurch kann eine schnellstmögliche Aufklärung des Sachverhalts, eine entsprechende Korrektur des Datensatzes des IKU bzw. der Gläubigerin sowie die Einstellung/Beendigung des Inkassoverfahrens gegen die irrtümlich in Anspruch genommene verwechselte Person herbeigeführt werden.

Erfahrungsgemäß erfolgt bei derartigen Fallkonstellationen eine umgehende Prüfung des Sachverhalts seitens des IKU sowie die Einstellung des Inkassoverfahrens gegenüber der betroffenen Person. Schließlich besteht seitens des IKU ein originäres Eigeninteresse daran, sich sowohl gesetzeskonform zu verhalten, als auch daran, die bestehende Forderung gegenüber dem/der tatsächlichen Schuldner/-in zu realisieren.

Grundsätzlich hat das IKU – bei Kenntniserlangung hinsichtlich einer Personenverwechslung – entsprechende Vorsorge zu treffen, eine Vermischung der Daten beider Personen zu vermeiden. Es empfiehlt sich daher beispielsweise, eine entsprechende Trennung der Datensätze vorzunehmen bzw. im Datensatz bzw. den Datensätzen des IKU die Daten der verwechselten Person als solche zu kennzeichnen, um weitere künftige Verwechslungen zu vermeiden.

Im Falle einer solchen Personenverwechslung besteht – neben dem Recht des/der tatsächlichen Schuldner/-in auf Auskunftserteilung – auch zu Gunsten der verwechselten Person ein Recht auf Auskunftserteilung nach Art. 15 DS-GVO gegenüber dem IKU.

Sofern nun die verwechselte Person Auskunft nach Art. 15 DS-GVO begehrt, ist seitens des IKU im Rahmen der Beauskunftung zwingend darauf zu achten, dass nicht die Daten des/der tatsächlichen Schuldners/-in (etwa dessen/deren Personalien, Rechnungsdaten etc.) an die verwechselte Person beauskunftet werden, sondern ausschließlich die Daten zu dieser verwechselten Person (beispielsweise deren Personalien sowie ggf. die Herkunft der Adressdaten der verwechselten Person (Wirtschaftsauskunftei, Adressdienstleister), sowie ggf. die Adressaten, an welche das IKU Daten der verwechselten Person übermittelt hat).

Dies gilt umgekehrt natürlich auch im Falle des Auskunftsersuchens des/der tatsächlichen Schuldners/-in: Hier dürfen seitens des IKU ausschließlich die

Daten, die zu dem/der Schuldner/-in verarbeitet werden, beauskunftet werden, nicht hingegen Daten betreffend der verwechselten Person.

Art. 15 DS-GVO lautet:

Art. 15 DS-GVO

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

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

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

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

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

Anhand der ihr gegenüber erteilten Auskunft wird nun die verwechselte Person – insbesondere durch die Nennung der Herkunft der Daten – letztlich in die Lage versetzt, beispielsweise Kontakt mit der Wirtschaftsauskunftei oder dem Adressdienstleister, der die unzutreffenden Adressdaten an das IKU übermittelt hat, aufzunehmen mit dem Hinweis, dass eine Personenver-

wechslung vorliegt und dort eine entsprechende Datenkorrektur zu erfolgen hat, um künftige Personenverwechslungen und damit fehlerhafte Auskunftserteilungen zu vermeiden.

Darüber hinaus bestehen zu Gunsten der verwechselten Person auch gegenüber der Wirtschaftsauskunftei oder dem Adressdienstleister entsprechende weitere Datenschutzrechte, wie etwas das Recht auf Auskunftserteilung nach Art. 15 DS-GVO. Auch anhand dieser Auskunft kann die verwechselte Person gegebenenfalls ermitteln, woher die ihre Person betreffenden Daten, die bei der Wirtschaftsauskunftei oder dem Adressdienstleister gespeichert sind, stammen.

In jedem Fall ist ein solches Tätigwerden seitens der betroffenen Person zu empfehlen. Ferner steht der verwechselten Person die Möglichkeit offen, sich an die für die betroffenen Unternehmen zuständigen Datenschutzaufsichtsbehörden zu wenden. Deren Zuständigkeit ergibt sich in der Regel jeweils daraus, in welchem Bundesland der (Haupt-)Firmensitz des Unternehmens im Handelsregister eingetragen ist. Diese Daten können häufig dem Impressum der Webseite des jeweiligen Unternehmens entnommen werden.

Weiterhin sind die Wirtschaftsauskunfteien oder Adressdienstleister gehalten, durch die erfolgten Rückmeldungen gegebenenfalls die bestehenden Datensätze zu korrigieren, um somit künftige Personenverwechslungen zu vermeiden. Darüber hinaus sollten diese anlassunabhängig die Qualität der Prozesse der Zuordnung der Datensätze regelmäßig überprüfen (beispielsweise durch Evaluation und Analyse etwaiger Fehlerquoten im Rahmen des Zuordnungs- und Beauskunftungsprozesses) und auf der Basis dieses Ergebnisses gegebenenfalls optimieren.

13. Internet, Werbung

13.1
Cookies auf dem Prüfstand – Länderübergreifende Tracking-Prüfung bei Zeitungs-Webseiten

Cookies sind für das Internet in der gewohnten Form unentbehrlich, werden allerdings häufig auch für datenschutzrechtlich problematische Dienste genutzt. Daher prüfe ich gemeinsam mit mehreren deutschen Aufsichtsbehörden ausführlich die entsprechende Praxis auf den Webseiten großer Zeitungsverlage.

Auffällige Hinweise und Pop-up-Fenster, in denen um Zustimmung zum Setzen von Cookies gebeten wird, sind seit einiger Zeit bei der Internetnutzung allgegenwärtig. Damit ist das Thema Cookies verstärkt in den Fokus der Öffentlichkeit gerückt. Die Nutzung von Cookies ist jedoch keineswegs neu, es gibt sie seit Mitte der 1990er-Jahre und damit aus Sicht der meisten Internetnutzer schon immer. Cookies sind Dateien, welche die Anbieter aufgerufener Webseiten auf dem Gerät des Nutzers ablegen und in denen sie bestimmte, individuelle Werte und Informationen speichern und bei fortgesetzter Nutzung wieder auslesen können. Dank dieser Technik können Informationen, Einstellungen oder Eingaben des Nutzers dauerhaft festgehalten werden (z. B. Spracheinstellungen, Inhalt eines Warenkorbs etc.).

Die Verwendung von Cookies ist häufig notwendig, um bestimmte, oft als selbstverständlich erachtete Funktionen von Webseiten technisch überhaupt zu ermöglichen. Von solchen technisch notwendigen Cookies geht in aller Regel keine große Gefahr für die Rechte und Freiheiten der betroffenen Nutzer aus. Die teilweise verbreitete Ansicht, Cookies seien generell gefährlich bzw. datenschutzrechtlich bedenklich, ist also nicht richtig.

Cookies werden, zusammen mit ähnlichen Technologien (z. B. Fingerprinting etc.), allerdings häufig auch dazu genutzt, die Nutzer einer (oder auch mehrerer) Webseite(n) zu verfolgen bzw. zu „tracken“. Dabei wird ein individuelles Nutzermerkmal erzeugt und gespeichert, anhand dessen der Nutzer bzw. das von ihm verwendete Gerät bei allen zukünftigen Nutzungen zuverlässig wiedererkannt werden kann. So kann das Verhalten des einzelnen Nutzers über einen langen Zeitraum hinweg und teilweise sehr detailliert beobachtet werden. Aus den gesammelten Informationen ergibt sich ein Nutzerprofil, das genaue Informationen über die Eigenschaften oder Vorlieben des jeweiligen Nutzers enthalten kann. Je nach Ausgestaltung des zugrundeliegenden Tracking-Verfahrens sind derartige Profile sehr umfassend und nicht auf einzelne Webseiten begrenzt. Dies gilt umso mehr, wenn zur Profilbildung

auf global agierende Dienstleister und deren Dienste zurückgegriffen wird, die das Nutzungsverhalten aus unterschiedlichen Nutzungskontexten zusammenführen und zu einem Profil aggregieren.

Trackingdienste spielen beispielsweise eine wichtige Rolle bei der Analyse und Optimierung des jeweiligen Webangebots (Webanalyse). Je genauer ein Webseitenbetreiber weiß, welche Nutzergruppen auf welche Weise bestimmte Bereiche seines Dienstes nutzen, desto eher kann er sein Angebot und die dort geschaltete Werbung daraufhin ausrichten. Mittels verschiedener Tools zur Webanalyse, die von diversen externen Dienstleistern angeboten werden, kann ein Webseitenbetreiber so ein umfassendes Bild von der Nutzung seiner Webseite erhalten.

Eine besonders große Bedeutung hat das Anlegen und Auswerten von Nutzerprofilen mittels Tracking aber für die Werbung. Durch die Profile wird eine möglichst individuelle und damit erfolgversprechende Ansprache des Nutzers mit für ihn potenziell relevanter Werbung ermöglicht. Wird beispielsweise an der gleichen Stelle einer Webseite einer jungen Mutter Werbung für Spielzeug, einem Senioren dagegen Werbung für Hörgeräte angezeigt, verspricht dies den Werbetreibenden sehr viel mehr Erfolg, als wenn alle Nutzer die gleiche Werbung für ein Produkt sehen, das für sie persönlich möglicherweise irrelevant ist. Entsprechend kann ein Werbeplatz mit personalisierter Werbung vom Anbieter der Webseite auch einträglicher vermarktet werden. Die entsprechenden Werbedienste werden in aller Regel nicht von den Betreibern der Webseiten selbst betrieben, sondern von einer Vielzahl von externen Dienstleistern, die für ihre Zwecke die Daten der Nutzer erheben und verarbeiten.

Rechtlich gibt es bei den Themen Cookies und Tracking leider viele Unklarheiten. Zusammen mit der DS-GVO sollte im Jahr 2018 eigentlich eine europäische ePrivacy-Verordnung mit speziellen Regeln zu Cookies und zum Tracking in Kraft treten. Aus politischen Gründen ist das Gesetzgebungsverfahren aber noch immer nicht abgeschlossen. Gleichzeitig werfen die daher noch immer geltende, inzwischen aber schon in die Jahre gekommene europäische ePrivacy-Richtlinie und deren deutsche Umsetzung im Telemediengesetz im Zusammenspiel mit den Regelungen der DS-GVO einige rechtliche Fragen auf. Diese konnten trotz mehrerer Urteile des EuGH und des BGH in den letzten Jahren nur teilweise geklärt werden. Vor diesem Hintergrund hat die Datenschutzkonferenz eine umfangreiche Orientierungshilfe für Anbieter von Telemediendiensten veröffentlicht, die die Ansichten der Aufsichtsbehörden widerspiegeln und den Anbietern Hilfestellungen zur rechtlichen Einordnung der verschiedenen Verarbeitungstätigkeiten geben (s. 48. Tätigkeitsbericht von 2019, 13.2).

Die Webseitenbetreiber bzw. Branchenverbände haben teilweise eigene Konzepte entwickelt, um Hinweise auf Cookies und das Einholen von Einwilligungen zur Datenverarbeitung möglichst einheitlich und nach eigener Auffassung rechtssicher zu gestalten. So wurde beispielsweise vom europäischen Digitalmarketing Branchenverband IAB Europe das sog. Transparency and Consent Framework (TCF) entwickelt, das auch von vielen deutschen Webseitenbetreibern eingesetzt wird. Mit diesem Rahmen soll die Kommunikation der verschiedenen Anbieter untereinander standardisiert und das Einholen von Einwilligungen über mehrere Anbieter hinweg vereinheitlicht und erleichtert werden. Ob dieser Standard tatsächlich auch den Anforderungen des europäischen Datenschutzrechts genügt, konnte bisher noch nicht abschließend geklärt werden, wird von vielen Aufsichtsbehörden aber bezweifelt.

Eine Branche, die besonders intensiv Werbeplätze vermarktet und zur Finanzierung ihrer häufig unentgeltlichen Angebote oft in besonderem Umfang Trackingdienste einsetzt, ist die Verlagsbranche mit den Webportalen ihrer Zeitungen und Zeitschriften. So setzen Zeitungswebseiten oft mehrere Trackingdienste verschiedener Dienstleister ein, um möglichst hohe Erlöse aus der dort platzierten Werbung zu erzielen.

Gemeinsam mit mehreren anderen deutschen Datenschutzaufsichtsbehörden führe ich daher in dieser besonders exponierten Branche eine länderübergreifende, koordinierte Datenschutzprüfung durch, um mir ein Bild von der Trackingpraxis großer Zeitungsunternehmen zu verschaffen und, falls nötig, unzulässige Praktiken zu unterbinden. Die beteiligten Behörden haben zusammen Fragebögen und ergänzende Unterlagen entwickelt, mit denen die geprüften Unternehmen aufgefordert wurden, ihre jeweilige Praxis bei der Nutzung von Trackingdiensten bzw. beim Setzen von Cookies darzulegen. Daneben wurden technische und rechtliche Prüfungsstandards festgelegt, um eine möglichst einheitliche Prüfung über die Bundesländer hinweg zu gewährleisten.

Ich habe im Rahmen der Prüfung mehrere große Zeitungsunternehmen aus Hessen angeschrieben und umfassende Auskünfte über deren Trackingpraxis eingeholt. Gleichzeitig wurden die jeweiligen Webangebote technisch gesichert und umfangreiche technische Analysen vorgenommen.

In der umfangreichen Prüfung werden nun gemeinsam mit den Aufsichtsbehörden der anderen beteiligten Bundesländer einheitliche Kriterien für die Aus- und Bewertung der Prüfungsergebnisse festgelegt. Auf diese Weise wird eine einheitliche und vergleichbare Auswertung der Ergebnisse bei allen Beteiligten ermöglicht. Nach Abschluss der Auswertung werde ich, wie sicherlich auch die Kollegen aus den anderen Bundesländern, konstruktiv,

falls nötig aber auch sanktionierend an die Betreiber der geprüften Dienste und Webseiten herantreten und ggf. notwendige Änderungen anstoßen.

Mit den bei der Prüfung, auch zusammen mit den Kollegen aus anderen Bundesländern, erarbeiteten Standards und gewonnenen Erkenntnissen wird gleichzeitig auch eine Grundlage für die zukünftige Prüfung weiterer Anbieter und Webseiten geschaffen. So kann langfristig eine rechtskonforme Praxis beim Tracking und beim Einsatz von Cookies sichergestellt werden.

13.2
Keine Werbung mit Corona-Daten!

Im Sommer des Berichtsjahres waren beim Besuch von Gaststätten nach den Vorschriften der Corona-Kontakt- und Betriebsbeschränkungsverordnung durch die Betriebsinhaberinnen und Betriebsinhaber der Name, die Anschrift und die Telefonnummer der Gäste zu erheben. Die Daten durften ausschließlich zur Ermöglichung der Nachverfolgung von Infektionen (Corona-Kontaktverfolgung) durch die hierfür zuständigen Behörden verwendet werden. Eine darüberhinausgehende Datenerhebung oder eine Verwendung der Daten zu anderen Zwecken wie z. B. für Werbung war unzulässig.

Aufgrund von § 4 Abs. 1 Nr. 2b der Verordnung zur Beschränkung von sozialen Kontakten und des Betriebs von Einrichtungen und von Angeboten aufgrund der Corona-Pandemie (Corona-Kontakt- und Betriebsbeschränkungsverordnung) vom 7. Mai 2020 in der Fassung der am 15. August 2020 in Kraft tretenden Änderungen durch Art. 3 der Siebzehnten Verordnung zur Anpassung der Verordnungen zur Bekämpfung des Corona-Virus vom 11. August 2020 waren die Betriebsinhaberinnen und Betriebsinhaber von Gaststätten und Übernachtungsbetrieben in Hessen verpflichtet, die Namen, Anschriften und Telefonnummern ihrer Gäste zu erheben. Die erhobenen Gästedaten waren einen Monat lang aufzubewahren bzw. zu speichern, durften Dritten nicht zur Kenntnis gelangen und waren ausschließlich zur Ermöglichung der Nachverfolgung von Infektionen (Corona-Kontaktverfolgung) durch die hierfür zuständigen Behörden vorgesehen.

§ 4 (Corona-Kontakt- und Betriebsbeschränkungsverordnung)

(1) Gaststätten im Sinne des Hessischen Gaststättengesetzes vom 28. März 2012 (GVBl. S. 50), zuletzt geändert durch Gesetz vom 15. Dezember 2016 (GVBl. S. 294), Mensen, Hotels, Kantinen, Eisdielen, Eiscafés und andere Gewerbe dürfen Speisen und Getränke (…)

(2) zum Verzehr vor Ort anbieten, wenn sichergestellt ist, dass

(…)

b) Name, Anschrift und Telefonnummer der Gäste ausschließlich zur Ermöglichung der Nachverfolgung von Infektionen von der Betriebsinhaberin oder dem Betriebsinhaber erfasst werden; diese haben die Daten für die Dauer eines Monats ab Beginn des Besuchs geschützt vor Einsichtnahme durch Dritte für die zuständigen Behörden vorzuhalten und auf Anforderung an diese zu übermitteln sowie unverzüglich nach Ablauf der Frist sicher und datenschutzkonform zu löschen oder zu vernichten; (…)

(…)

Zur Erfüllung dieser Vorschrift wurden in vielen Restaurants und Gasstätten Datenerhebungsformulare an die Gäste verteilt, die alle nach dem Erhebungszeitpunkt sortiert aufzubewahren waren. Nach dem ersten Monat waren jeden Tag diejenigen Datenerhebungsbögen zu vernichten, für die die Aufbewahrungsfrist von einem Monat abgelaufen war. In vielen größeren und gut besuchten Betrieben sammelten sich auf diese Weise sehr viel zusätzliche Papierunterlagen an, für deren sichere Aufbewahrung erheblicher Platz benötigt und Aufwand betrieben wurde. Um Platz zu sparen, Aufwand zu reduzieren, die Gefahr der Einsichtnahme Dritter zu minimieren und nach einem Monat der Vernichtungsverpflichtung stets pünktlich nachkommen zu können, wurden bereits kurze Zeit nach Wirksamwerden der Corona-Kontakt- und Betriebsbeschränkungsverordnung immer mehr automatisierte Systeme in Form von Smartphone-Apps oder Online-Anwendungen zur Erhebung und Speicherung der Gästedaten durch die Gastwirte und Restaurantbetreiber eingesetzt.

Durch den Hinweis eines Gastes wurde ich auf ein solches automatisiertes System zur Datenerfassung aufmerksam, bei dem ein hessisches Restaurant seine Gäste über einen auf jedem Tisch angebrachten QR-Code, der mit dem Smartphone einzuscannen war, auf ein Online-Datenerhebungsformular lenkte. In diesem Online-Datenerhebungsformular, das nach dem darüber angebrachten Text eigentlich lediglich dazu dienen sollte, die erhobenen Daten dem Gesundheitsamt zur Verfügung zu stellen, falls eine Infektionskette nachverfolgt werden muss, war von dem Restaurantbetreiber neben den für die Corona-Nachverfolgung vorgeschriebenen Datenerhebungsfeldern „Name“, „Anschrift“ und „Telefonnummer“ zusätzlich das Datenerhebungsfeld „E-Mail“ angebracht worden. Unter dem Formular befand sich ein Zusatztext „Ich genehmige bis zum Widerruf, dass meine Daten zu Marketingzwecken von dem Restaurant und Verbundunternehmen benutzt werden können“. Vor diesem Einwilligungstext für Werbung war ein Optionsfeld platziert, das bereits mit einem Haken vorbelegt war.

Umgehend nach Eingang des Hinweises auf diese Datenerhebungspraxis und die beabsichtigte Nutzung von Corona-Nachverfolgungsdaten zu Werbezwecken habe ich den Restaurantbetreiber darauf hingewiesen, dass die zur Bekämpfung der Corona-Pandemie zu erhebenden Daten grundsätzlich ausschließlich zum Zweck der Corona-Nachverfolgung genutzt werden dürfen. Einer werblichen Verwendung der erhobenen Daten steht die, der Vorschrift deutlich zu entnehmende strikte Zweckbindung der Daten entgegen. Zudem gehören E-Mail-Adressen nicht zu den nach der Corona-Kontakt- und Betriebsbeschränkungsverordnung zu erhebenden Daten und dürfen daher auch auf der Grundlage dieser Vorschrift nicht erhoben werden.

Für eine wirksame Werbe-Einwilligung wäre es außerdem erforderlich, dass aus dem Einwilligungstext klar hervorgeht, um welche Verbundunternehmen des Restaurantbetreibers es hier geht, zu welchen Branchen diese Unternehmen gehören und ob der Betroffene in Werbung per Briefpost, E-Mail, Telefon oder SMS einwilligt. Der unter dem Datenerhebungsformular angebrachte Einwilligungstext war für eine rechtswirksame Einwilligung in Werbung also viel zu unbestimmt und hinsichtlich des beabsichtigten Werbemediums zu undifferenziert.

Hinzu kam, dass für eine wirksame Einwilligung gem. Art. 4 Nr. 11 DS-GVO und ErwG 32 Satz 3 eine eindeutige, aktive, bestätigende Handlung des Betroffenen erforderlich wäre:

Artikel 4 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

(…)

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

(…)

Erwägungsgrund 32

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung. Dies könnte etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder durch eine andere Erklärung oder Verhal-

tensweise geschehen, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen.

(…)

Da das zu dem Einwilligungstext angebrachte Optionsfeld bereits mit einem Haken vorbelegt war, war eine eindeutige bestätigende Handlung des Gastes zur Erteilung einer Werbe-Einwilligung gar nicht mehr möglich. Vorbelegte Einwilligungslösungen, die keine aktive Handlung von Betroffenen mehr erfordern, führen daher stets zur Unwirksamkeit der Einwilligungen.

Dem Unternehmen, das das Restaurant betrieb und auch für die Online-Datenerhebung verantwortlich war, wurde verdeutlicht, dass aufgrund der Unwirksamkeit der bisher erteilten Einwilligungen alle bereits mit diesem Verfahren erhobenen E-Mail-Adressen von Gästen zu löschen sind.

Außerdem habe ich dem Unternehmen dringend nahegelegt, den ohnehin untauglichen Einwilligungstext, das zugehörige vorbelegte Optionsfeld sowie das Datenerhebungsfeld für die E-Mail-Adresse aus dem Erhebungsformular zu entfernen. Denn auch wenn die Vorbelegung des Optionsfeldes entfernt und ein wirksamer Einwilligungstext angebracht würde, der den Anforderungen an Klarheit und Bestimmtheit einer Einwilligung genügt, und zusätzliche Auswahlfelder für das gewünschte Werbe-Medium (Postbrief, E-Mail, Telefon, SMS) angebracht würden, würde dies aufgrund der je nach Verwendungszweck der Daten unterschiedlichen Ansprüche (u. a. an die Möglichkeit der Kenntnisnahme durch Dritte und die Fristen für eine Datenlöschung) eine ganze Reihe sowohl organisatorischer als auch datenschutzrechtlicher Probleme nach sich ziehen, die extremen Aufwand verursachen würden und dennoch kaum rechtlich sauber zu lösen wären.

Das Unternehmen hat daraufhin das Datenerhebungsfeld „E-Mail“ sowie den ungenügenden Einwilligungstext und das Optionsfeld vollständig und ersatzlos aus dem Online-Datenerhebungsformular entfernt. Die bis zu diesem Zeitpunkt erhobenen E-Mail-Adressen waren noch nicht zum Versand von Werbe-E-Mails verwendet worden und wurden vollständig gelöscht.

14. Technik, Organisation

14.1
Übermittlung personenbezogener Daten per E-Mail

Für die Kommunikation sowohl mit als auch zwischen öffentlichen und nichtöffentlichen Stellen ist der Einsatz von E-Mails weit verbreitet und hat während der SARS-CoV2-Pandemie noch an Bedeutung gewonnen. Von Verantwortlichen sind die Vorgaben der Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DS-GVO zu erfüllen, wenn Kommunikationsinhalte oder -metadaten einen Personenbezug aufweisen. Für den Kernbereich der Übermittlung hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) auf ihrer 99. Sitzung eine Orientierungshilfe (OH) verabschiedet. Die Umsetzung dieser OH erfordert, dass alle an der Kommunikation beteiligten Akteure ihren Beitrag leisten.

Am 12. Mai 2020 verabschiedete die DSK die im AK Technik erarbeitete OH „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“, s. a. Anhang I 3.1. Diese fokussiert auf Anforderungen zur Umsetzung der Vorgaben des Art. 5 Abs. 1 lit. f sowie der Art. 25 und 32 Abs. 1 DS-GVO. Die erfolgreiche Umsetzung dieser Anforderungen kann nur im Zusammenspiel aller Akteure gelingen.

Zum besseren Verständnis wird zunächst der Ablauf der E-Mail-Kommunikation schematisch dargestellt. Es werden hierbei nur diejenigen Aspekte berücksichtigt, die für die weiteren Ausführungen in diesem Beitrag relevant sind. Die Darstellung bildet die Basis, um im Anschluss näher auf die an der E-Mail-Kommunikation beteiligten Akteure und ihre wechselseitigen Abhängigkeiten einzugehen. Hierauf aufbauend wird separat auf die wesentlichen Anforderungen an die einzelnen Akteure eingegangen.

Schematischer Ablauf der E-Mail-Kommunikation

Die Abbildung 1 bietet einen schematischen Überblick über die für diesen Beitrag relevanten Aspekte der E-Mail-Kommunikation.

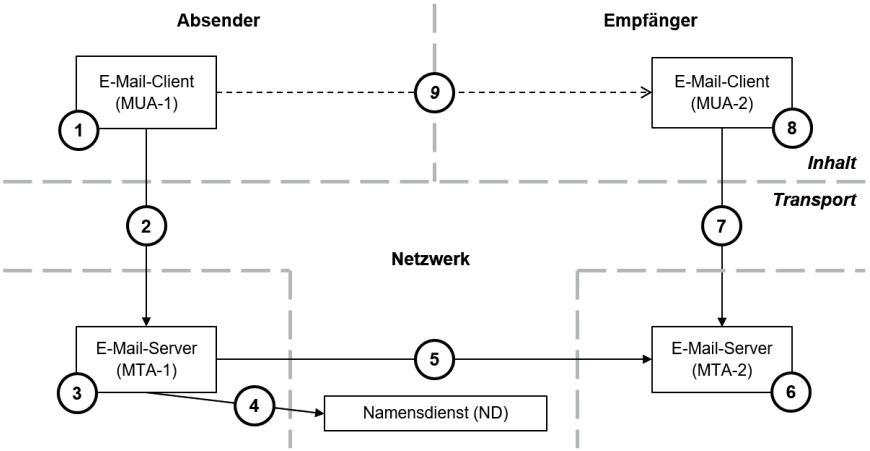


Abbildung 1: Schematisch Darstellung der E-Mail-Kommunikation

Sie stellt exemplarisch den Ablauf der Übermittlung einer E-Mail von einem menschlichen *Absender* zu einem menschlichen *Empfänger* dar. Hierbei wird davon ausgegangen, dass Absender und Empfänger unterschiedlichen Verantwortlichen im Sinne der DS-GVO angehören, etwa zwei unabhängigen Unternehmen. Außerdem muss die zu übermittelnde E-Mail zwischen zwei separaten E-Mail-Servern über ein oder mehrere Netzwerke übertragen werden.

Dieses Szenario dient als Grundlage der weiteren Ausführungen. Ein wesentliches Merkmal ist hierbei, dass die Auswahl des Empfängers sowie die Erstellung des Inhalts jeweils bewusst durch eine Person erfolgen. Weitere mögliche Szenarien werden im Folgenden nicht näher betrachtet, etwa der Versand automatisiert generierter E-Mails ohne menschliches Eingreifen oder der Versand von E-Mail, innerhalb des Einflussbereichs eines einzelnen Verantwortlichen.

An der E-Mail-Kommunikation sind die folgenden relevanten Komponenten beteiligt.

– **E-Mail-Client des Absenders (MUA-1)** – Ein E-Mail-Client, im Englischen Mail User Agent (MUA), dient einem Absender zur Erstellung der E-Mail und zu deren Abschicken. Hierbei kann es sich bspw. um ein auf dem Computer des Absenders installiertes E-Mail-Programm oder um eine Web-basierte Nutzerschnittstelle handeln.

– **Sendender E-Mail-Server (MTA-1)** – Dieser Server bzw. IT-Dienst, im Englischen Mail Transfer Agent (MTA), nimmt vom MUA-1 zum Versand bestimmte E-Mails entgegen und sorgt für deren Übermittlung an die nächste Station.
– **Namensdienst (ND)** – Ein Namensdienst dient der Ermittlung relevanter Informationen, etwa über empfangende E-Mail-Server für eine konkrete E-Mail-Adresse.
– **Empfangender E-Mail-Server (MTA-2)** – Dieser Server bzw. IT-Dienst nimmt E-Mails entgegen und hält sie für den Abruf durch E-Mail-Clients von Empfängern bereit.
– **E-Mail-Client des Empfängers (MUA-2)** – Dieser E-Mail-Client wird vom Empfänger zum Abruf und zur Darstellung von E-Mails verwendet. Analog zu MUA-1 sind hier ebenfalls unterschiedliche Realisierungen möglich.

Durch die in Abbildung 1 enthaltene Nummerierung kann der schematische Ablauf der E-Mail-Kommunikation nachvollzogen werden.

1. Der Absender verfasst eine E-Mail unter Verwendung von Funktionalitäten des MUA-1 und versieht die E-Mail mit der E-Mail-Adresse des Empfängers.
2. Mittels entsprechender Funktionalitäten von MUA-1 wird die fertige E-Mail über ein Netzwerk an MTA-1 übertragen. Bei diesem Netzwerk kann es sich bspw. um ein Firmennetzwerk oder das Internet handeln. Eine Übertragung über mehrere Netzwerkgrenzen hinweg ist ebenfalls möglich.
3. Nach der Entgegennahme der E-Mail wird diese von MTA-1 gespeichert. Diese Speicherung und die hiermit verbundenen datenschutzrechtlichen Anforderungen werden hier nicht näher betrachtet, da sie nicht der eigentlichen Übermittlung zuzurechnen sind. Sie sind jedoch vom Verantwortlichen ebenfalls zu erfüllen.
4. MTA-1 ermittelt über ein Netzwerk von einem Namensdienst die (Netzwerk-)Adresse des MTA-2, sofern diese nicht bereits bekannt ist. Bei dem Netzwerk handelt es sich i. d. R. um das Internet.
5. MTA-1 überträgt die E-Mail auf Basis der im vorangegangenen Schritt ermittelten Adresse an MTA-2. Die Übertragung erfolgt ebenfalls über ein Netzwerk.
6. Nach der Entgegennahme der E-Mail wird diese von MTA-2 gespeichert und zum Abruf für den Empfänger über dessen MUA vorgehalten. Analog zu Schritt 3 werden diese Speicherung und die hiermit verbundenen Anforderungen in diesem Beitrag nicht weiter betrachtet.
7. Mittels entsprechender Funktionalitäten von MUA-2 wird die E-Mail über ein Netzwerk von MTA-2 abgerufen. Analog zu Schritt 2 kann es sich

bei diesem Netzwerk bspw. um ein Firmennetzwerk, das Internet oder sogar um mehrere Netzwerke handeln.

8. Der Empfänger liest die E-Mail unter Zuhilfenahme der von MUA-2 hierzu bereitgestellten Funktionalitäten.

Die horizontale Linie zwischen Inhalt und Transport dient der Darstellung der konzeptionellen Trennung zwischen ebendiesen beiden Ebenen der E-Mail-Kommunikation.

Auf der Inhaltsebene stellt Schritt 1 somit das Verfassen des E-Mail-Inhaltes auf Absenderseite dar. Schritt 8 stellt analog das Lesen bzw. die Verarbeitung des E-Mail-Inhaltes auf Empfängerseite dar. Durch Schritt 9 wird verdeutlicht, dass die eigentliche, inhaltliche Kommunikation zwischen Sender und Empfänger erfolgt. Auf dieser Ebene ist auch eine etwaige Ende-zu-Ende-Verschlüsselung angesiedelt.

Die Schritte 2, 4, 5 und 7 bilden jeweils eine Kommunikation auf der Transportebene ab. Eine solche Kommunikation erfolgt über ein oder mehrere Netzwerke. Hierbei ist zu beachten, dass es sich i. d. R. um unterschiedliche Netzwerke handelt. So kann bspw. der Versand einer E-Mail zwischen MUA-1 und MTA-1 über ein Firmennetzwerk erfolgen, falls der Verantwortliche einen eigenen E-Mail-Server innerhalb seines Netzwerks betreibt. Demgegenüber kann die Übertragung der E-Mail von MTA-1 zu MTA-2 über das Internet erfolgen. Eine direkte Übertragung zwischen MTA-1 und MTA-2 ist nicht der Regelfall. Vielmehr sind häufig mehrere Zwischenstationen beteiligt. Diese sind jedoch für diesen Beitrag von nachrangiger Bedeutung. Bei der Übertragung zwischen den einzelnen Zwischenstationen sollte jeweils eine Transportverschlüsselung zum Einsatz kommen.

Auf Namensdienste wird im Folgenden nicht näher eingegangen. Sie spielen jedoch im Rahmen der Erfüllung konkreter Anforderungen der OH eine wichtige Rolle, etwa im Zusammenhang mit einer qualifizierten Transportverschlüsselung in Kapitel 5.2.

Als Grundlage der E-Mail-Kommunikation dient somit eine durch Offenheit und Dezentralität gekennzeichnete Infrastruktur. So können Verantwortliche bspw. ein oder mehrere an der Kommunikation beteiligte Komponenten selbst betreiben. Zur konkreten Umsetzung stehen ihnen diverse Möglichkeiten zur Verfügung. So ist etwa eine Vielzahl alternativer Implementierungen unterschiedlicher Hersteller als Grundlage für den Betrieb von MTAs verfügbar.

Akteure der E-Mail-Kommunikation

Die Anforderungen zum Schutz personenbezogener Daten im Rahmen der E-Mail-Kommunikation richteten sich an die unterschiedlichen an der

Kommunikation beteiligten Akteure. In diesem Beitrag werden die folgenden Akteure unterschieden.

I. **E-Mail-Provider** – Hierbei handelt es sich um Anbieter von E-Mail-Infrastrukturen. Diese bieten sie ihren Kunden an, etwa in Form von E-Mail-Postfächern und zugehörigen Web-basierten Verwaltungsschnittstellen. Auch können Web-basierte MUAs Bestandteil der Angebote von E-Mail-Providern sein. Häufig sind die Angebote von E-Mail-Providern mehr oder minder standardisiert.

II. **Organisation als Kunde eines E-Mail-Providers** – Hierbei handelt es sich um institutionelle Kunden von E-Mail-Providern.

III. **Organisation mit eigener E-Mail-Infrastruktur** – Organisationen, die selbst eine E-Mail-Infrastruktur betreiben, fallen in diese Gruppe von Akteuren.

IV. **Endnutzer** – Endnutzer sind Personen, die E-Mail als Kommunikationsmittel nutzen und die einer Organisation als Verantwortlichem angehören. Bei den Endnutzern handelt es sich um die bereits im Rahmen des Ablaufs der E-Mail-Kommunikation vorgestellten Absender und Empfänger. In diesem Beitrag wird nicht näher auf die private E-Mail-Nutzung eingegangen, etwa durch Kunden eines Unternehmens.

Organisation II und III sind im Kontext dieses Beitrags als Verantwortliche gemäß Art. 24 DS-GVO anzusehen. E-Mail-Provider agieren als Auftragsverarbeiter gemäß Art. 28 DS-GVO.

In Abbildung 2 werden die Akteure und ihre Beziehungen untereinander schematisch für den Fall dargestellt, dass eine verantwortliche Organisation auf die E-Mail-Infrastruktur eines E-Mail-Providers zurückgreift.

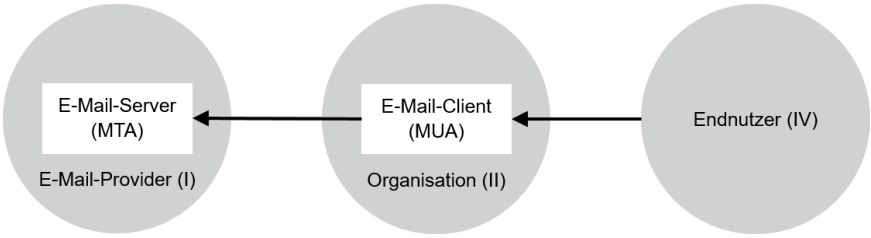


Abbildung 2: Einbeziehung E-Mail-Provider

Die graue Hervorhebung dient der Abgrenzung des Einflussbereichs des jeweiligen Akteurs. Diesen Einflussbereichen sind die bereits in Abbildung

1 dargestellten Komponenten E-Mail-Client (MUA) und E-Mail-Server (MTA) zugeordnet.

Die Zuordnung dient der Herstellung von Bezügen zwischen den Einflussbereichen der einzelnen Akteure und den Komponenten der E-Mail-Kommunikation. Sie richtet sich nach der Kontrolle über die jeweiligen Komponenten. So wird bspw. in Abbildung 2 der von einer Organisation II genutzte MTA von einem E-Mail-Provider betrieben. Dementsprechend ist der MTA dem Einflussbereich des E-Mail-Providers zugeordnet. Hiervon unberührt bleiben etwaige Konfigurationsmöglichkeiten, die Organisation II vom E-Mail-Provider in Bezug auf MTAs eingeräumt werden.

Analog hierzu bildet Abbildung 3 Akteure, Komponenten und Einflussbereiche im Falle des vollständigen Eigenbetriebs der Infrastruktur durch eine verantwortliche Organisation ab.

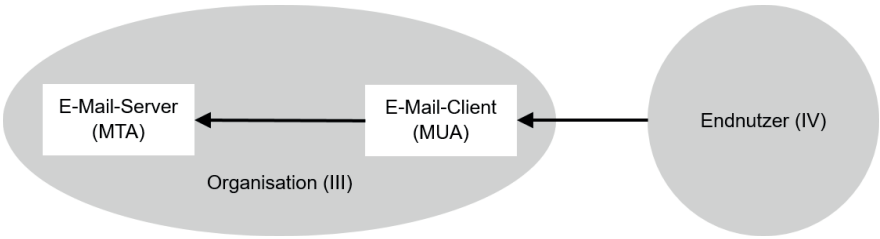


Abbildung 3: Eigenbetrieb

Im Folgenden wird auf die Einflussbereiche der einzelnen Akteure näher eingegangen.

I. E-Mail-Provider

Durch die Zuordnung eines MTA zum Einflussbereich eines E-Mail-Providers wird hervorgehoben, dass ein E-Mail-Provider zumindest die wesentlichen Aspekte der seinen Kunden bereitgestellten MTAs festlegt. Hierzu zählen u. a. die Ausgestaltung der zugrundeliegenden IT-Infrastruktur, die Auswahl der eingesetzten Software und die Vornahme entsprechender Konfigurationseinstellungen. Die Zuordnung zum Einflussbereich des E-Mail-Providers bedeutet nicht, dass eine Organisation II keinen Einfluss auf den MTA nehmen kann. So kann ein E-Mail-Provider einer Organisation II bspw. eine Web-basierte Verwaltungsschnittstelle zur Verfügung stellen, über die sie Teile des Verhaltens der eingesetzten MTAs beeinflussen kann.

Beim Versand von E-Mails über einen MTA bestehen Abhängigkeiten hinsichtlich der Ausgestaltung des korrespondierenden MTA auf Empfangsseite. Diese ergeben sich z. B. aus den vom empfangenden MTA unterstützten Möglichkeiten zur Transportverschlüsselung. Umgekehrt gilt dies auch für den Empfang von E-Mails.

II. Organisation als Kunden eines E-Mail-Providers

Art und Umfang der für Organisation (II) bereitgestellten Möglichkeiten zur Konfiguration und Beeinflussung des Verhaltens eines von einem E-Mail-Provider betriebenen MTA können stark variieren. Im datenschutzrechtlichen Kontext sind hier vor allem Möglichkeiten zur Festlegung, Umsetzung und Anwendung technischer und organisatorischer Maßnahmen im Sinne des Art. 32 DS-GVO von besonderer Bedeutung. Hierbei wird mit der Auswahl eines E-Mail-Providers bzw. eines Angebots desselben bereits der Rahmen für das von Organisation II als Verantwortlichem gewährleistbare Schutzniveau in Bezug auf den oder die MTAs festgelegt.

Der von einem Endnutzer verwendete MUA ist in Abbildung 2 dem Einflussbereich der zugehörigen Organisation zugeordnet. Hierdurch wird hervorgehoben, dass die Organisation die Ausgestaltung des MUA bestimmt. In der Regel wird von einer Organisation festgelegt, welche Software als MUA zum Einsatz kommt. Diese Software wird von der Organisation entsprechend konfiguriert den Endnutzern der Organisation bereitgestellt. Hierdurch bestimmt die Organisation den wesentlichen Rahmen für die E-Mail-Nutzung durch ihre Endnutzer.

Bei der Ausgestaltung dieses Rahmens ist Organisation II sowohl vom weiter oben durch den E-Mail-Provider festgelegten Rahmen als auch von ergänzenden Maßnahmen abhängig, die nicht ausschließlich im MUA realisiert werden können. Hierzu zählt z. B. die Schaffung der Voraussetzungen zum Einsatz einer Ende-zu-Ende-Verschlüsselung. In diesem Zusammenhang ist eine Organisation II auch von der Unterstützung kompatibler Verfahren durch diejenigen Verantwortlichen abhängig, mit denen Ende-zu-Ende-verschlüsselt kommuniziert werden soll.

III. Organisation mit eigener E-Mail-Infrastruktur

Wie in Abbildung 3 dargestellt, liegen sowohl MTA als auch MUA im Einflussbereich einer Organisation mit eigener E-Mail-Infrastruktur (III). Hieraus ergibt sich, dass eine solche Organisation beide Bestandteile der E-Mail-Kommunikation weitestgehend unter Kontrolle hat. Dementsprechend hat die Organisation, im Vergleich zu den Erläuterungen in den beiden vor-

angegangenen Abschnitten, ein höheres Maß an Freiheiten hinsichtlich der Ausgestaltung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO. Dies gilt insbesondere in Bezug auf die Abhängigkeit von einem E-Mail-Provider. Gleichzeitig ist häufig mit einem höheren Aufwand im Vergleich zum Einsatz eines E-Mail-Providers zu rechnen.

Die Ausführungen zu E-Mail-Providern hinsichtlich der Abhängigkeiten von den MTAs der Kommunikationspartner beim Senden und Empfangen von E-Mails gelten in gleicher Weise.

IV. Endnutzer

Endnutzer verwenden einen von einer Organisation (I oder II) bereitgestellten MUA zum Verfassen, zum Versand sowie zum Abruf und zum Lesen von E-Mails. Wie in den Abbildungen 2 und 3 dargestellt, liegt der verwendete MUA nicht im Einflussbereich des Endnutzers. Dies bedeutet nicht, dass Endnutzer keinen Einfluss auf datenschutzrechtliche Aspekte bei der Übermittlung von E-Mails haben. Die Einflussmöglichkeiten sind jedoch durch die von der Organisation festgelegten Rahmenbedingungen abhängig. Sind bspw. von Seiten der Organisation die Voraussetzungen für eine Ende-zu-Ende-Verschlüsselung geschaffen worden, so kann ein Endbenutzer diese grundsätzlich für die E-Mail-Kommunikation nutzen. Die Schaffung der Voraussetzungen ist hierbei nicht auf den MUA begrenzt. Gleichwohl muss die Ende-zu-Ende-Verschlüsselung auch vom MUA unterstützt werden.

Die Möglichkeit zur Nutzung der von der zugehörigen Organisation bereitgestellten Rahmenbedingungen hängt häufig zusätzlich von der Empfängerseite ab. Nur wenn auch auf dieser die nötige Voraussetzung geschaffen wurden, können die bereitgestellten Maßnahmen auch tatsächlich zum Einsatz kommen. So setzt der Einsatz einer Ende-zu-Ende-Verschlüsselung bspw. voraus, dass beide Seiten diese auf kompatible Weise unterstützen.

Anforderungen an die Akteure

Auf Basis der Erläuterungen in den vorangegangenen Abschnitten wird im Folgenden auf die resultierenden Anforderungen an die einzelnen Akteure eingegangen. Hierbei wird nicht mehr zwischen Organisationen mit und ohne Einbeziehung eines E-Mail-Providers unterschieden.

I. E-Mail-Provider

E-Mail-Provider müssen bei der Ausgestaltung ihrer Angebote die Anforderungen ihrer Kunden berücksichtigen. Nur wenn sie ihren Kunden den Anforderungen entsprechende E-Mail-Infrastrukturen bereitstellen, werden diese

überhaupt erst in die Lage versetzt, gemäß Art. 32 DS-GVO erforderliche Maßnahmen zu ergreifen. Dementsprechend kommt E-Mail-Providern eine zentrale Rolle bei der Schaffung von Voraussetzungen für die Umsetzung datenschutzrechtlicher Anforderungen zu.

Um es bspw. Verantwortlichen zu ermöglichen, gemäß Kapitel 4.2.1 der OH einem normalen Risiko in Bezug auf die Vertraulichkeit gerecht zu werden, muss ein E-Mail-Provider eine obligatorische Transportverschlüsselung unterstützen. Besser als eine strikte Umsetzung wäre die Bereitstellung von Einflussmöglichkeiten für Verantwortliche, etwa eine selektive Deaktivierung für einzelne Domänen oder E-Mail-Adressen. Idealerweise könnten Endnutzer beim Versand einer E-Mail über ihren MUA selbst festlegen, ob eine obligatorische Transportverschlüsselung zur Anwendung kommen soll oder nicht.

Ein Verantwortlicher, der auf einen E-Mail-Provider zurückgreift, ist bei der Ausgestaltung seiner E-Mail-Infrastruktur stark auf den vom E-Mail-Provider vorgegebenen Rahmen festgelegt. Durch diese Rahmenbedingungen legt der E-Mail-Provider im Wesentlichen fest, welche Maßnahmen vom Verantwortlichen umsetzbar sind. Dementsprechend beeinflusst ein E-Mail-Provider auch mittelbar den Handlungsspielraum von Endnutzern. Die Rahmenbedingungen können von E-Mail-Provider zu E-Mail-Provider und von Angebot zu Angebot variieren.

II. Organisation

Organisationen ist dringend angeraten, im Falle der Nutzung eines E-Mail-Providers bereits bei dessen Auswahl geplante und erforderliche Maßnahmen zu berücksichtigen. Hierzu zählt insbesondere auch die Durchführung einer Risikobetrachtung für die Einsatzszenarien der E-Mail-Kommunikation. Aus den resultierenden Ergebnissen lassen sich entsprechende Anforderungen an Angebote von E-Mail-Providern ableiten, die daraufhin als Kriterien bei der Auswahl eines E-Mail-Providers bzw. dessen Angebots in Kombination mit den übrigen Auswahlkriterien angewendet werden.

Verantwortliche müssen die Zusicherungen der E-Mail-Provider prüfen und hierbei ihre gemäß Art. 28 Abs. 3 lit. h DS-GVO eingeräumten Möglichkeiten nutzen. Die Umsetzung einer obligatorischen Transportverschlüsselung ist bspw. unverzichtbar, um zu gewährleisten, dass auch tatsächlich transportverschlüsselt kommuniziert wird. Demgegenüber deuten Analysen in meinem IT-Laboratorium darauf hin, dass im Zweifelsfall eine Transportverschlüsselung nicht zur Anwendung kommen muss, selbst wenn diese vermeintlich von den beteiligten MTAs unterstützt werden würde. Gründe hierfür können bspw. Inkompatibilitäten oder Fehlersituationen sein.

Beim Eigenbetrieb der E-Mail-Infrastruktur durch Verantwortliche sind im Wesentlichen die gleichen Aspekte wie beim Rückgriff auf einen E-Mail-Provider zu berücksichtigen. Zusätzlich sind technische und organisatorische Maßnahmen für Bereitstellung, Betrieb und Wartung der Infrastruktur zu ergreifen. Durch den Eigenbetrieb kann der im Vergleich zum Einsatz eines E-Mail-Providers i. d. R. größere Entscheidungsspielraum und die für Eigenbetrieb spezifischen Rahmenbedingungen eine wesentliche Rolle spielen, etwa die Kontrolle über die eingesetzte Infrastruktur.

Darüber hinaus müssen weitere technische Maßnahmen ergriffen werden, etwa in Bezug auf die Auswahl und Konfiguration des den Endnutzern bereitgestellten MUA. Auch hierbei ist der Verantwortliche in wesentlichen Bereichen von den durch einen etwaigen E-Mail-Provider gesetzten Rahmenbedingungen abhängig. Dies gilt z. B. für Möglichkeiten zur Anbindung von MUAs an MTAs.

Zusätzlich sollten Kommunikationspartner bei der Umsetzung ihrer technischen und organisatorischen Maßnahmen unterstützt werden. Dies sollte durch die Schaffung der notwendigen Voraussetzungen erfolgen, etwa durch eine Unterstützung entsprechender Standards für eine qualifizierte Transportverschlüsselung (Kapitel 5.2 der OH) oder die Unterstützung einer Ende-zu-Ende-Verschlüsselung (Kapitel 5.3 der OH).

Es ist nicht ausreichend, wenn Verantwortliche technische Rahmenbedingungen für den datenschutzrechtskonformen Einsatz der E-Mail-Kommunikation schaffen. Zusätzlich müssen von ihnen gemäß Art. 32 DS-GVO auch organisatorische Maßnahmen ergriffen werden. Hierzu zählen insbesondere die Festlegung von Vorgaben bei der Nutzung der bereitgestellten Plattform durch Endnutzer. Auch müssen Endnutzer entsprechend sensibilisiert und geschult werden.

Zu beachten ist hierbei insbesondere, dass den Endnutzern umsetzbare Vorgaben gemacht werden müssen. So dürfte es Endnutzern i. d. R. nicht möglich sein, eine Transportverschlüsselung sicherzustellen, falls technisch keine obligatorische Transportverschlüsselung unterstützt wird.

Die ergriffenen Maßnahmen müssen gemäß Art. 32 Abs. 1 lit. d DS-GVO hinsichtlich ihrer Wirksamkeit zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig überprüft, bewertet und evaluiert werden.

Schließlich müssen potenzielle Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO identifiziert und entsprechend behandelt werden. So ergaben Analysen statistischer Daten zu ausgehendem E-Mail-Verkehr in meinem IT-Laboratorium Indizien für potenzielle Verletzungsszenarien. Beispiele hierfür waren

– der Versand nicht-transportverschlüsselter E-Mails an Kommunikationspartner, für die mindestens ein normales Risiko hinsichtlich der Vertraulichkeit von personenbezogenen Inhalten naheliegt,
– der nicht-transportverschlüsselte Versand von E-Mails an Kommunikationspartner, für die eine Transportverschlüsselung zu erwarten wäre und
– der Versand von E-Mails, bei denen bei der Adressierung der Empfänger offensichtlich Schreibfehler unterlaufen sind.

In allen diesen Fällen sind weiterführende Analysen erforderlich.

III. Endnutzer

Der Handlungsspielraum von Endnutzern ist durch die vom Verantwortlichen bereitgestellte E-Mail-Infrastruktur festgelegt. Dies gilt sowohl in technischer Hinsicht als auch in Bezug auf die ihnen gemachten Vorgaben für die Nutzung der bereitgestellten Infrastruktur. Hinzu kommen die spezifischen Gegebenheiten der Kommunikationspartner, etwa die Unterstützung einer Ende-zu-Ende-Verschlüsselung.

Endnutzer müssen bei der Nutzung von E-Mail als Mittel der Kommunikation den ihnen gegebenen Handlungsspielraum angemessen nutzen. So müssen sie i. d. R. beim beabsichtigten Versand einer E-Mail zunächst das vorhandene Risiko für Rechte und Freiheiten betroffener Personen bestimmen und im Anschluss entsprechend verfahren, etwa durch Einsatz einer Ende-zu-Ende-Verschlüsselung im Einklang mit Kapitel 4.2.2 der OH im Falle des Vorliegens eines hohen Risikos beim Bruch der Vertraulichkeit von Inhaltsdaten.

Fazit

Die von der DSK verabschiedete OH liefert eine gute Basis zur Ausgestaltung technischer und organisatorischer Maßnahmen, um die Anforderungen der DS-GVO an den Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu gewährleisten. Die offene und dezentrale Architektur als Grundlage der E-Mail-Kommunikation, der optionale Einsatz ergänzender Standards sowie die Vielzahl an Kommunikationspartnern und Abhängigkeiten zwischen diesen führen zu nicht unerheblichen Herausforderungen hinsichtlich der Umsetzung dieser Anforderungen.

Verantwortliche müssen ihre Endnutzer durch die Ergreifung technischer und organisatorischer Maßnahmen in die Lage versetzen, die bereitgestellte E-Mail-Infrastruktur datenschutzrechtskonform nutzen zu können. Bei Hinzuziehung eines E-Mail-Providers ist die frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen schon bei der Provider-Auswahl von

besonderer Bedeutung. Wesentliche nachträgliche Anpassungen am durch den ausgewählten E-Mail-Provider gesetzten Rahmen dürften nur noch schwer möglich sein. Gleiches gilt auch bei der Realisierung einer selbst betriebenen E-Mail-Infrastruktur. Zwar hat ein Verantwortlicher hier die Kontrolle über die eingesetzte IT-Infrastruktur, aber auch hier dürften nachträgliche Änderungen mit wesentlich höheren Aufwänden verbunden sein.

Organisationen und E-Mail-Provider sind aufgerufen, die Voraussetzungen zu schaffen, um den Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu gewährleisten. Dies schließt insbesondere auch die Unterstützung ergänzender Standards mit ein, wie in der OH der DSK referenziert. Die Unterstützung derartiger Standards erfolgt hierbei nicht zum Selbstzweck. Vielmehr bilden sie nicht zuletzt auch eine notwendige Voraussetzung, um Kommunikationspartner ihrerseits in die Lage zu versetzen, die Anforderungen an den Schutz personenbezogener Daten bei der Übermittlung per E-Mail zu gewährleisten.

14.2
Weitere Referenzmaßnahmen zum Standard-Datenschutzmodell

Das Standard-Datenschutzmodell (SDM) sowie Referenzmaßnahmen bieten Verantwortlichen und Auftragsverarbeitern Orientierung, welche technisch-organisatorischen Maßnahmen zu ergreifen sind, um eine Verarbeitung personenbezogener Daten datenschutzkonform zu gestalten, bereitzustellen, zu betreiben und vorzuhalten. Entsprechende Beiträge hinsichtlich der fortschreitenden Entwicklung des SDM finden sich zudem im 47. (Ziff. 4.10.1) und im 48. Tätigkeitsbericht (Ziff. I 14.4).

Entwicklung des Standard-Datenschutzmodells (SDM)

Im November 2019 ist eine neue Version des SDM-Handbuchs durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ohne Gegenstimme verabschiedet worden. Dabei wurde der Lebenszyklus eines Datenschutzmanagements in das Handbuch integriert und die entsprechende Referenzmaßnahme aufgelöst, die im 47. Tätigkeitsbericht gesondert dargestellt war. Wesentliche Artikel in der DS-GVO zur technischen Bewertung einer Verarbeitung personenbezogener Daten sind erläutert. Ausführungen zu Grundlagen eines Datenschutzmanagements, wie das Planen oder das Spezifizieren, das Kontrollieren oder das Prüfen, das Beurteilen und das Verbessern von technisch-organisatorischen Maßnahmen für Verarbeitungstätigkeiten sind entsprechend im 48. Tätigkeitsbericht dargestellt.

Das SDM umfasst das erwähnte Handbuch und wird schrittweise um Referenzmaßnahmen ergänzt. Jede Referenzmaßnahme beinhaltet eine Darstellung einer technisch-organisatorischen Maßnahme, mittels derer eine datenschutzkonforme Verarbeitung zu gewährleisten ist.

Im Jahr 2020 wurden weitere Referenzmaßnahmen veröffentlicht, die häufig auch als Bausteine bezeichnet werden. Die neuen Bausteine beziehen sich auf das „Aufbewahren", das „Berichtigen", das „Einschränken einer Verarbeitung" und das „Trennen" als Konkretisierungen von Schutzmaßnahmen zur datenschutzkonformen Umsetzung von Verarbeitungstätigkeiten. Die nun gewählten Bezeichnungen für diese Maßnahmen sollen verdeutlichen, dass in der konkreten Umsetzung datenschutzrechtlicher Anforderungen verschiedene Aktivitäten bei den Verantwortlichen oder den Auftragsverarbeitern erforderlich sind. So ist technisch-organisatorisch sicherzustellen, dass Maßnahmen regelmäßig im Betrieb der Systeme und Dienste auf Dauer einer regelmäßigen Revision unterzogen werden. Dies ist im bereits referenzierten Datenschutzmanagement angelegt. Zudem sind die Referenzmaßnahmen „Dokumentieren", „Löschen und Vernichten" und „Protokollieren" entsprechend angepasst worden.

Diese Veröffentlichungen, weitere Bausteine sowie ggf. Aktualisierungen können auf der Webseite des SDM unter *https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/* (letzter Aufruf: 06.11.2020) nachgelesen werden, die vom bundesweiten Arbeitskreis Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder betrieben wird.

Fazit und Perspektive

Das SDM-Handbuch bietet grundsätzlich durch die Beschreibung von Schutzmaßnahmen Orientierung, was insbesondere aus Sicht des Technischen Datenschutzes zur Umsetzung von Verarbeitungstätigkeiten zu tun ist. Schutzmaßnahmen sind zu ergreifende technische und organisatorische Maßnahmen, die eine datenschutzkonforme Umsetzung der jeweiligen Verarbeitungstätigkeit sicherstellen sollen. Mittels der Referenzmaßnahmen bzw. der Bausteine werden Hinweise gegeben, welche Maßnahmen technisch-organisatorisch konkret für Systeme und Dienste und deren Betrieb auf Dauer bereitzustellen und vorzuhalten sind. Auf diese Weise können jeweils Verarbeitungsvorgänge datenschutzkonform realisiert werden, die Komponenten von spezifischen Verarbeitungstätigkeiten sind. Aus technischer Sicht sind solche Komponenten bzw. Verarbeitungsvorgänge somit datenschutzrechtlich hinsichtlich ihrer Eignung und möglicher Angemessenheit zu bewerten.

Das SDM befindet sich auf einem guten Weg, wechselseitig die Abhängigkeiten zwischen datenschutzrechtlichen Anforderungen und zu implementierenden Schutzmaßnahmen darzulegen. Umgekehrt lassen sich ergriffene technisch-organisatorische Maßnahmen durch die Referenzmaßnahmen bzw. Bausteine hinsichtlich ihrer Wirksamkeit überprüfen, womit auch ein Beitrag zur Anwendung von Art. 32 Abs. 1 lit. d DS-GVO geleistet wird.

Perspektivisch wird im Rahmen datenschutzrechtlicher Zertifizierungen ähnliches zu betrachten sein, siehe hierzu speziell 47. Tätigkeitsbericht, in dem Anforderungen an Akkreditierungen von Zertifizierungsstellen und an datenschutzrechtliche Zertifizierungen gemäß Art. 42 und Art. 43 DS-GVO in Grundzügen dargestellt sind. Gemäß der nach Art. 43 Abs. 1 lit. b DS-GVO anzuwendenden technischen Norm EN ISO/IEC 17065 erfordert die Folgenorm DIN ISO/IEC 17067 die Festlegung von Prüfkriterien, Prüfsystematik und -methoden. Datenschutzrechtliche Anforderungen sind grundsätzlich Prüfkriterien. Weiter bedarf es einer Prüfsystematik, die durch die generischen Schutzmaßnahmen des SDM für den Technischen Datenschutz abgedeckt werden kann. Ferner können die bereits vorhandenen Bausteine zusätzlich Anforderungen an benötigte Prüfmethoden speisen.

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

15.1 Meldungen nach Art.33 DS-GVO in Zeiten der Corona-Pandemie

Fehlversand, Hackerangriffe sowie Verlust und Diebstahl von Datenträgern und Unterlagen bleiben die häufigsten Ursachen für die Meldungen von Verletzungen des Schutzes personenbezogener Daten in Hessen. Die Corona-Pandemie hinterlässt jedoch auch bei den Datenpannen und dem Meldeverhalten der verantwortlichen Stellen sichtbare Spuren.

Mit insgesamt 1.433 Meldungen bleibt die Zahl der mir gegenüber angezeigten Datenschutzverletzungen im Berichtsjahr auf dem bereits im Vorjahr (1.453 Meldungen) erreichten hohen Niveau, s. a. Teil I Ziff. 17.1 und 17.2. Bei der Mehrzahl der gemeldeten Datenpannen ging es erneut um den Fehlversand per Post, E-Mail oder Fax, Hackerangriffe einschließlich Phishing- und Schadsoftwarevorfälle sowie Verlust und Diebstahl von Datenträgern und Unterlagen. Aus diesem Grund fasse ich die wichtigsten zu beachtenden Aspekte bei diesen typischen Fallkonstellationen noch einmal kurz zusammen.

Fehlversand von Daten

Die häufigste Ursache der an mich gemeldeten Datenschutzverletzungen nach Art. 33 DS-GVO war der Fehlversand von Daten. Die meisten dieser Vorfälle betrafen Gesundheits-, Beschäftigten- oder Kundendaten und beruhen oft auf individuellen menschlichen oder technischen Fehlern. In diesen Fällen haben mir die verantwortlichen Stellen zugesichert, dass entsprechende Maßnahmen, wie Mitarbeiterfortbildungen sowie Überprüfung und Anpassung von internen Prozessen, ergriffen wurden, um das erneute Vorkommen solcher Vorfälle zu verhindern.

Hackerangriffe, Phishing, Schadsoftware

Ein weiterer wesentlicher Teil der Meldungen aus dem Berichtsjahr befasste sich mit kriminellen Zugriffen von außen in Form von Hacker-, Phishing- und Schadsoftwareattacken. In diesem Kontext ist es mir wichtig, erneut darauf hinzuweisen, dass zwecks Abwehr solcher unrechtmäßigen Angriffe bereits im Vorfeld entsprechende geeignete technische und organisatorische Maßnahmen zu ergreifen sind. Diese sind insbesondere unter Berücksichtigung des aktuellen Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände, der Zwecke und des Risikos der Verarbeitung zu

treffen, um ein angemessenes Schutzniveau zu erreichen (vgl. Art. 32 Abs. 1 DS-GVO). Darüber hinaus halte ich ein unverzügliches und effektives Handeln zur Schadensbeseitigung bzw. -minimierung, z. B. durch Analyse von infizierten Systemen, Zurücksetzen von kompromittierten Passwörtern, Durchführen von Updates, aber auch Kontaktaufnahme zu relevanten Behörden und den Betroffenen, für unabdingbar.

In meinem 48. Tätigkeitsbericht 2019 berichtete ich unter Ziffer 4.3 bereits ausführlich über den Umgang mit Phishing-Vorfällen. Die dort erläuterten Grundsätze in Bezug auf die technischen und organisatorischen Vorkehrungen und Maßnahmen sind auch bei anderen Arten von Außenangriffen heranzuziehen.

Verlust oder Diebstahl von Datenträgern und Unterlagen

Im Berichtsjahr wurden in vielen Fällen Sachverhalte an mich herangetragen, bei denen Unterlagen, Pakete oder USB-Sticks auf dem Postweg verloren gegangen sind. Darüber hinaus führten Einbrüche mit Diebstahl von Geräten und Dokumenten zum Erstatten einer entsprechenden Meldung an meine Behörde. Auch zur Vermeidung solcher Fallkonstellationen muss ein Sicherheits- und Datenschutzkonzept mit umfassenden technischen und organisatorischen Maßnahmen implementiert werden. Bei Hardwaregeräten ist es vor allen Dingen eine sichere Verschlüsselung der Festplatte nach den aktuellen Standards, die stets überprüft werden soll. In übrigen Fällen tragen Maßnahmen der Sicherung von Gebäuden und Räumlichkeiten (Warnanlage, aufbewahrungssichere, abschließbare Räume und Schränke, Tresore) sowie Sensibilisierung der Mitarbeiter zu einer datenschutzkonformen Lösung bei.

Auswirkungen der Corona-Pandemie

Neben den bereits bekannten Problemstellungen machte sich, wie in allen anderen Bereichen, auch bei den Meldungen nach Art. 33 DS-GVO die aktuelle Corona-Situation bemerkbar. Besonders zu Beginn der Pandemie konnten viele verantwortlichen Stellen ihrer Meldepflicht nicht innerhalb der vom Verordnungsgeber vorgesehenen Frist von 72 Stunden (vgl. Art. 33 Abs. 1 DS-GVO) ab Kenntnisnahme des Vorfalls nachkommen. Einige Meldungen wurden mit Verspätung eingereicht. Die Verantwortlichen begründeten dies unter anderem damit, dass sich viele Beschäftigten in Home-Office oder Kurzarbeit befanden und dies zu Verzögerungen in den Abläufen führte. Die Verzögerungen ergaben sich dadurch, dass zunächst neue Arbeitsweisen integriert und viele Abläufe neu organisiert werden mussten. Hinzu kamen z. B. technische Hürden, begrenzte Erreichbarkeit sowie das zum Teil hohe

Corona-bedingte Arbeitsaufkommen der zuständigen Mitarbeiter aus den betroffenen Bereichen.

Da die diesbezüglichen Ausführungen der verantwortlichen Stellen gut begründet und nachvollziehbar waren und die 72-Stunden-Frist nicht unverhältnismäßig überschritten wurde, sah ich bei den bisher abschließend geprüften Fällen von einer Sanktionierung ab.

Das aktuelle Geschehen rund um die Corona-Pandemie spiegelte sich jedoch nicht nur bei den Meldefristen, sondern auch bei den gemeldeten Sachverhalten selbst wider. So erreichten mich mehrere Meldungen von Verantwortlichen aus dem öffentlichen und nicht öffentlichen Bereich, bei denen die Daten über eine Covid-19-Erkrankung z. B. durch Arbeitgeber, Schule oder Arztpraxis unzulässiger Weise unbeabsichtigt entweder offengelegt oder an einen falschen Empfänger übermittelt wurden. Darüber hinaus liegen mir einzelne Meldungen über die Verwechslung von Testergebnissen im Rahmen eines Corona-Tests vor. Zwei der gemeldeten Vorfälle fanden im Rahmen der Errichtung von Corona-Impfzentren und der damit verbundenen Mitarbeiterakquise statt. Einzelne Datenpannen ereigneten sich im Rahmen der Nutzung von Videokonferenzen oder der Weiterleitung von dienstlichen Daten an private Endgeräte (z. B. durch Risikopatienten, um von zuhause aus arbeiten zu können). Bei diesen Fällen wurden von den verantwortlichen Stellen die erforderlichen Schritte eingeleitet, um den gegebenenfalls entstandenen Schaden zu beseitigen. Die Betroffenen wurden gemäß Art. 34 DS-GVO über die Datenschutzverletzungen informiert.

Abschließend ist festzuhalten, dass durch die Corona-Pandemie im Vergleich zum vorangegangenen Berichtszeitraum keine besonders schwerwiegenden Verletzungen des Schutzes personenbezogener Daten gemeldet wurden und keine Erhöhung der Zahl der gemeldeten Datenschutzverstöße zu verzeichnen ist. Es ist jedoch festzustellen, dass in der aktuellen Situation deutlich intensiver und oft unter Zeitdruck sensible Gesundheitsdaten, die zu den besonderen Kategorien personenbezogener Daten i. S. von Art. 9 DS-GVO gehören, verarbeitet werden. Da diese Daten besonders schützenswert sind, sind ein erhöhtes Maß an Sorgfalt im Umgang mit den Daten sowie besondere präventive Maßnahmen in der aktuellen Zeit mehr denn je erforderlich.

15.2
Meldung von Datenschutzpannen bei der Polizei – Anwendung des § 60 HDSIG in der Praxis

Seit Gültigkeit des HDSIG (25. Mai 2018) besteht auch eine Meldepflicht für Verletzungen des Schutzes personenbezogener Daten im Bereich der Richtlinie (EU) 2016/680.

Beispiele für meldepflichtige Sachverhalte:

– Ein Bediensteter der Polizei fragt ohne dienstlichen Bezug in zahlreichen Fällen mehrere Familienangehörige im polizeilichen Informationssystem und im Melderegister ab.
– Ein Bediensteter der Polizei fragt seine geschiedene Ehefrau im Melderegister ab, um wegen des Familienzuschlags zu erfahren, ob diese wieder verheiratet ist.
– Eine Bedienstete der Polizei möchte ein Jahrgangstreffen organisieren und fragt mehrere Personen im Melderegister ab, um die aktuellen Anschriften zu erlangen.
– Eine Mutter konfrontiert den Freund ihrer Tochter damit, dass er ein „Drogendealer“ sei und sie ihrer Tochter daher den weiteren Umgang mit ihm verboten habe. Der Vater arbeitet bei der Polizei und hatte im polizeilichen Informationssystem nach dem Freund seiner Tochter recherchiert und das Ergebnis seiner Frau mitgeteilt.
– Eine Bedienstete der Polizei möchte eine Wohnung vermieten und überprüft die Interessenten im polizeilichen Informationssystem, da sie die Wohnung nur an eine unbescholtene Person vermieten möchte.
– Eine Bedienstete der Polizei wird von einer Freundin gebeten, ihr eine Halteranschrift zu einem Fahrzeug nach einem angeblich von ihr verursachten Bagatellunfall zu besorgen. Tatsächlich handelt es sich aber um das Auto der neuen Lebensgefährtin des Ex-Mannes ihrer Freundin, das einige Nächte später zerkratzt und schwer beschädigt wird.

Die Meldepflicht gem. § 60 HDSIG besteht für öffentliche Stellen des Landes Hessen im Anwendungsbereich des dritten Teils des HDSIG bzw. § 40 HDSIG, der die Richtlinie (EU) 2016/680 umsetzt. Adressaten der Norm sind insbesondere die Hessische Polizei, die Hessische Justiz, das Hessische Landesamt für Verfassungsschutz, aber auch Bußgeldstellen und Kommunen, soweit sie im Rahmen der Verfolgung von Ordnungswidrigkeiten tätig sind.

§ 60 HDSIG

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Hessischen Datenschutzbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung nach Abs. 1 hat zumindest folgende Informationen zu enthalten:

1. *eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,*
2. *den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,*
3. *eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und*
4. *eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.*

(4) Wenn und soweit die Informationen nach Abs. 3 nicht zur gleichen Zeit bereitgestellt werden können, hat der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Abs. 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 37 Abs. 4 findet entsprechende Anwendung.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

Eine Verarbeitung personenbezogener Daten findet in besonderem Maße, qualitativ wie quantitativ, bei der Hessischen Polizei statt. Deren Tätigkeit erlaubt im Bereich der strafverfolgenden sowie präventiven Sachbearbeitung eine Verarbeitung personenbezogener Daten in großem Umfang. Neben den Daten aus der Sach- bzw. Vorgangsbearbeitung betreibt die Hessischen Polizei ein landesweites polizeiliches Informationssystem (POLAS-Hessen), in dem auch Daten aus Strafverfahren zu präventiven Zwecken gespeichert werden

dürfen. Weiterhin bestehen, soweit die individuelle Tätigkeit dies erfordert, Zugangsmöglichkeiten auf weitere Dateisysteme und auch das Melderegister. Die Arbeit der Polizei erfordert dabei eine Berechtigungsstruktur, die einer großen Anzahl Bediensteter einen schnellen und komfortablen Zugriff auf diese Daten ermöglicht.

Nicht erst mit den in der Öffentlichkeit bekanntgewordenen missbräuchlichen und damit rechtswidrigen Abfragen in diesen Systemen wurde offenbar, dass die tatsächlichen Möglichkeiten in Einzelfällen von Bediensteten über die rechtliche Zulässigkeit hinaus genutzt werden.

Da es sich i. d. R. um besonders schützenswerte Daten handelt, muss bei einer rechtswidrigen Abfrage immer geprüft werden, ob ein meldepflichtiger Verstoß gem. § 60 HDSIG im Verantwortungsbereich des betreffenden Polizeipräsidiums vorliegt.

Gem. § 60 Abs. 1 HDSIG als nicht meldepflichtig sind Verletzungen des Schutzes personenbezogener Daten einzustufen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Dem Verantwortlichen wird damit zunächst eine Prognose abgefordert, die regelmäßig mehr Hintergrundinformationen erfordert als die bloße Tatsache, dass der Bedienstete A die Person B nachvollziehbar in einem Dateisystem abgefragt hat. Soweit also innerhalb der gesetzlich gebotenen Frist keine Informationen erlangt werden können, die zu einem Risikoausschluss führen, wird regelmäßig eine Meldung an meine Behörde erfolgen müssen.

Abfragen in polizeilichen oder polizeilich zugänglichen Dateisystemen erfolgen in großem Umfang, denen verschiedenste Auslösekonstellationen zugrunde liegen. Exemplarisch wäre hier die klassische Verkehrskontrolle zu nennen, weiterhin aber auch Überprüfungen im Zusammenhang mit Fahndungen und Ermittlungen.

In einem ersten Schritt kann i. d. R. über Plausibilitätsprüfungen festgestellt werden, ob die Abfrage im Zusammenhang mit einer konkreten polizeilichen Befassung erfolgte oder nicht. Falls keine dokumentierte Befassung erkennbar/nachvollziehbar ist, bestehen weiterhin zahlreiche Fallkonstellationen, in denen die/der Bedienstete die Abfrage/n trotzdem im Rahmen seiner dienstlichen Tätigkeit und damit rechtmäßig vorgenommen haben kann. Eine diesbezügliche Überprüfung ist jedoch oftmals nur unter Einbeziehung der/des betreffenden Bediensteten möglich. Soweit die Bewertungen ergeben, dass nicht von einer rechtmäßigen Datenabfrage auszugehen ist, muss im Einzelfall die bereits oben erwähnte Prognose erfolgen.

Ein Risiko für die Rechte und Freiheiten natürlicher Personen wird grundsätzlich zu bejahen sein, wenn erhobene Daten an Dritte weitergegeben wurden, unabhängig davon, ob es Daten zu einer polizeilichen Befassung sind oder auch melderechtliche Daten. Dies ist durchaus nicht immer der Fall und oft auch nur schwer nachweisbar.

Die Vorschrift des § 60 Abs. 1 HDSIG verpflichtet die verantwortliche Stelle weiterhin, einen festgestellten Verstoß innerhalb von 72 Stunden nach Bekanntwerden an meine Behörde zu melden. Hierfür stehen auf meiner Internetseite Formulare zur Verfügung.

In zahlreichen Fällen meldeten sich die Datenschutzbeauftragten der hessischen Polizeipräsidien mit der Frage, wann der Zeitpunkt des Bekanntwerdens anzunehmen sei, um fristgerecht eine Meldung gem. § 60 HDSIG zu machen.

Aufgrund der Heterogenität der zugrundeliegenden Sachverhalte kann dieser Zeitpunkt nicht allgemeingültig festgelegt werden. Vielmehr wird dem diesbezüglich Beauftragten der verantwortlichen Stelle abverlangt, zeitnah den Grad an Wahrscheinlichkeit zu erlangen, um eine sachgerechte Entscheidung im Hinblick auf die Auslösung einer Meldung treffen zu können. Dies wird immer dann der Fall sein, wenn der Verantwortliche über ein begründetes Maß an Gewissheit verfügt, dass der Vorfall zur Gefährdung personenbezogener Daten geführt hat. Der verantwortlichen Stelle wird dabei ein kurzer Zeitraum zur Untersuchung zuzugestehen sein, um festzustellen, ob eine Verletzung vorliegt oder nicht. Eine hohe Eintrittswahrscheinlichkeit für eine Verletzung der Rechte und Freiheiten natürlicher Personen sowie die mögliche Schwere etwaiger Folgen wird regelmäßig eine frühzeitige Meldung erforderlich machen.

Sofern Meldungen nicht oder nicht fristgerecht erfolgen, kann dies aufsichtsbehördliche Maßnahmen nach § 14 Abs. 2, 3 HDSIG nach sich ziehen. Im Jahr 2020 habe ich die nicht bzw. nicht fristgerecht erfolgte Meldung in mehreren Fällen beanstandet.

Die Informationen, die eine Meldung nach § 60 HDSIG beinhalten muss, sind in § 60 Abs. 3 HDSIG aufgeführt. Nicht aufgeführt und damit nicht Inhalt einer solchen Meldung sind in der Regel personenbezogene Daten, mit Ausnahme ggf. der Namen und Kontaktadressen der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen. Demnach erfordert die gesetzliche Regelung nicht die Meldung der Daten von „Täter“ und „Opfer“, mithin nicht der personenbezogenen Daten der/des rechtswidrig handelnden Bediensteten und der betroffenen Person. Das Meldeverfahren nach § 60 HDSIG hat nur zwei beteiligte Stellen, die datenschutzrechtlich verantwortliche Stelle und meine Behörde.

Von diesem Verfahren ist daher ein individuelles und personenbezogenes Sanktionsverfahren meiner Behörde in ihrer Funktion als Verfolgungsbehörde abzugrenzen. Ein solches Verfahren kann jedoch mittelbar durch eine Meldung nach § 60 HDSIG an mich ausgelöst werden. Dies ist immer dann der Fall, wenn der gemeldete Sachverhalt darauf hinweist, dass ein/e Bedienstete/r der verantwortlichen Stelle sich über ihre/seine innerdienstlich geregelten Befugnisse in Form eines sog. Mitarbeiterexzesses (siehe 48. Tätigkeitsbericht, S. 129 ff.) hinwegsetzte und ihr/sein Handeln damit nicht mehr der verantwortlichen Stelle zugerechnet werden kann. Diese/r Bedienstete kann dann in seiner datenschutzrechtlichen Bewertung den Regelungen der DS-GVO unterfallen und damit auch mit einem Bußgeld sanktioniert werden.

16. Bußgeldverfahren, Gerichtsverfahren

16.1
Bußgeldverfahren im Jahr 2020

Wiederholte Verstöße gegen die Vorschriften über die Betroffenenrechte führen zu hohen Bußgeldern. Aber auch Mitarbeiterexzess im öffentlichen und nicht öffentlichen Bereich stellt weiterhin ein wesentliches datenschutzrechtliches Problem in Hessen dar.

Einer Vielzahl der von mir im Berichtszeitraum durchzuführenden Ordnungswidrigkeitenverfahren lagen unzulässige Datenverarbeitungen durch Mitarbeiter öffentlicher und nicht öffentlicher Stellen zu privaten Zwecken – der sog. Mitarbeiterexzess – zugrunde (s. a. Teil I Ziff. 17.2). Insbesondere kam es in der Vergangenheit oft vor, dass Beschäftigte öffentlicher Stellen unrechtmäßig Daten in dienstlichen Systemen abriefen und diese dienstlich erlangten Informationen zu privaten Zwecken nutzten. So habe ich im Berichtsjahr in 22 Ordnungswidrigkeitenverfahren gegen Bedienstete der hessischen Polizei sowie zwei Verfahren gegen Mitarbeiterinnen und Mitarbeiter von Jobcentern in Hessen eingeleitet. Die meisten dieser Vorgänge befinden sich noch im Ermittlungs- bzw. Anhörungsstadium.

Die Anzahl der Verfahren gegen Bedienstete der hessischen Polizei wurde zum Anlass genommen, in Zusammenarbeit mit dem Hessischen Ministerium des Innern und für Sport sowie der einzelnen Polizeipräsidien die Abläufe im Ermittlungsverfahren zu verbessern. Ich rechne daher mit einem zügigen Abschluss dieser Fälle.

Ein weiterer wesentlicher Teil der von mir eingeleiteten Verfahren befasste sich mit den Verletzungen von Betroffenenrechten nach Kapitel III der DS-GVO. Bezüglich dieser Problematik wurden im Berichtsjahr insgesamt 13 neue Verfahren anhängig.

Auch Sachverhalte im Zusammenhang mit der aktuellen Corona-Pandemie waren Gegenstand der von mir zu ahndenden Ordnungswidrigkeitenverfahren. Oft ging es bei diesen Fällen um eine zweckwidrige Verwendung von Daten, die mittels sogenannter „Corona-Listen“ erhoben wurden. In einzelnen Verfahren, bei denen die Schwere des Verstoßes sowie die gesamten Umstände des Falls dies zuließen, entschied ich mich aus Opportunitätsgründen gemäß § 47 OWiG für die Sanktionierung mittels einer Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO statt der Verhängung eines Bußgeldes. Dies nicht zuletzt aufgrund der eingetretenen außergewöhnlichen Situation und der angespannten finanziellen Lage der betroffenen verantwortlichen Stellen.

Bußgeld wegen Zweckentfremdung von Daten im Rahmen eines Corona-Tests

Nach Erstattung einer Strafanzeige durch die betroffene Person und Abgabe des Verfahrens durch die Staatsanwaltschaft wurde ich mit einem Fall befasst, bei dem es um Mitarbeiterexzess im nicht öffentlichen Bereich ging. Der Vorfall ereignete sich in einem Unternehmen, das in einem Testzentrum COVID-19-Tests durchführt. Der betroffene Mitarbeiter kontaktierte kurz nach dem Test eine junge Dame über WhatsApp, um sie kennenzulernen. Der Verantwortliche gab sich als Mitarbeiter des Unternehmens zu erkennen und schwärmte von deren „Ausstrahlung", die auch der Grund für die verfahrensgegenständliche Kontaktaufnahme war. Im Rahmen der durchgeführten Ermittlungen konnte die Identität des Mitarbeiters zweifelsfrei festgestellt werden.

Der besagte Mitarbeiter verwendete vorliegend die im Rahmen der Durchführung eines Corona-Tests von der Anzeigeerstatterin angegebenen Daten zu privaten Zwecken und verstieß damit gegen das Zweckbindungsgebot Art. 5 Abs. 1 lit. b DS-GVO. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Kontaktdaten der Patienten im Rahmen des Corona-Testverfahrens sind ausschließlich zu dem Zweck zu erheben und aufzubewahren, um diese Personen über das Testergebnis zu informieren und gegebenenfalls in einem positiven Fall eine Kontaktaufnahme seitens der zuständigen Gesundheitsbehörde zu ermöglichen. Die Nutzung dieser Daten zu anderen Zwecken ist unzulässig. Die verfahrensgegenständliche Kontaktaufnahme per WhatsApp war vorliegend zur Erfüllung der von dem Beschuldigten zu erbringenden Aufgaben nicht erforderlich. Ein Ausnahmetatbestand nach Art. 6 Abs. 4 DS-GVO war nicht einschlägig. Auch lag eine Einwilligung der Anzeigeerstatterin in die Verwendung ihrer Daten zu anderen Zwecken zu keinem Zeitpunkt vor.

Der vorliegende Verstoß war nicht dem Kreis der unternehmerischen Tätigkeit des Arbeitgebers zuzurechnen. Der Mitarbeiter beging die ordnungswidrige Handlung zwar von seinem Arbeitsplatz aus, unter Einsatz der ihm zur Verfügung stehenden Arbeitsmittel, jedoch nicht in Ausübung seiner beruflichen Tätigkeit, sondern ausschließlich zu privaten Zwecken.

Der Verstoß wurde von mir gemäß Art. 83 Abs. 5 lit. a DS-GVO i. V. m. Art. 5 Abs. 1 lit. b DS-GVO mit einem Bußgeld von 300,00 € geahndet. Bei der Bußgeldzumessung wurde berücksichtigt, dass lediglich eine Person von dem in Rede stehenden Sachverhalt betroffen war und nur wenige Daten zweckwidrig verwendet wurden. Darüber hinaus war zu Gunsten des Verantwortlichen zu sehen, dass bislang keine datenschutzrechtlichen Beanstandungen gegen

ihn vorlagen. Im Rahmen der Anhörung im Ordnungswidrigkeitenverfahren machte der Betroffene keinerlei Angaben. Aufgrund der vorliegenden Erkenntnisse wurde das Nettoeinkommen geschätzt und als Grundlage für die Bußgeldbemessung herangezogen. Unter Berücksichtigung aller maßgeblichen Umstände erschien im Einzelfall eine Geldbuße im unteren Bereich des Bußgeldrahmens des Art. 83 Abs. 5 DS-GVO mit 300,00 € als wirksam, hinreichend abschreckend und verhältnismäßig. Der Bußgeldbescheid ist noch nicht rechtskräftig.

In meinem 48. Tätigkeitsbericht berichtete ich unter Ziffer 15.1 bereits umfassend über den Mitarbeiterexzess im öffentlichen Bereich. Anhand des hier beschriebenen Falls wird deutlich, dass diese Art des ordnungswidrigen Handels auch im nicht öffentlichen Bereich präsent ist und für eigenmächtig handelnde Mitarbeiter von Unternehmen aus der freien Marktwirtschaft diesbezüglich die gleichen Grundsätze gelten.

Bußgeld wegen wiederholter Verstöße gegen die Auskunftspflicht

Gegen eine kleine Kapitalgesellschaft mit Sitz in Hessen erreichten mich mehrere Beschwerden von Bürgern, bei denen es um Verletzungen der Betroffenenrechte nach Art. 15 i. V. m. Art. 12 DS-GVO ging. Nachdem zwei dieser Beschwerden abschließend im Aufsichtsverfahren geprüft und Verstöße bejaht wurden, leitete ich ein Bußgeldverfahren ein. In einem Fall verlangte der Beschwerdeführer die Erteilung einer Auskunft nach Art. 15 DS-GVO sowie die Löschung seiner Daten nach Art. 17 DS-GVO. Nach der Durchführung der Authentifizierung wurde ihm jedoch lediglich mitgeteilt, dass nur Daten gespeichert seien, die er selbst eingegeben habe. In der Folge wurden die Daten gelöscht, so dass die verlangte Auskunft nicht mehr erteilt werden konnte. In dem zweiten Fall wurde das Auskunftsbegehren des Beschwerdeführers zunächst nicht bearbeitet. Erst nach Einschreiten meiner Behörde wurde der Eingebende – mit einer Verspätung von mehr als drei Monaten – beauskunftet.

In beiden Fällen wurde von der verantwortlichen Stelle entgegen Art. 15 DS-GVO keine Auskunft zu den personenbezogenen Daten der betroffenen Person innerhalb der Frist des Art. 12 Abs. 3 S. 1 DS-GVO erteilt. Die beiden Verstöße wurden von mir nach Art. 83 Abs. 5 lit. b i. V. m. Art. 15 i. V. m. Art. 12 Abs. 3 S. 1 DS-GVO mit einem Bußgeldbescheid über einen mittleren fünfstelligen Betrag geahndet. Bei der Bußgeldzumessung wurde der herausgehobenen Bedeutung der Ordnungswidrigkeit sowie dem mittleren Schweregrad des Verstoßes Rechnung getragen. Das allgemein häufig ausgeübte Auskunftsrecht aus Art. 15 DS-GVO nimmt im Rahmen der Betroffenenrechte eine herausgehobene Stellung ein und stellt eine unverzichtbare Voraussetzung

für die Geltendmachung weiterer datenschutzrechtlicher Ansprüche dar. Zu Gunsten des verantwortlichen Unternehmens wirkte sich u. A. aus, dass jeweils lediglich ein Kunde von den Vorfällen betroffen war, darüber hinaus der Sachverhalt eingeräumt und bedauert wurde sowie das Verfahren überdurchschnittlich lang dauerte.

Bußgelderhöhend war dagegen zu berücksichtigen, dass sich die beiden verfahrensgegenständlichen Verstöße kurz hintereinander ereigneten. Dies deutete auf einen systematischen Fehler bzw. ein organisatorisches Problem im Unternehmen und ein erhöhtes Maß an Pflichtwidrigkeit des Verantwortlichen hin. Hierfür sprach, dass in beiden Fällen das rechtmäßige Vorgehen bei der Bearbeitung von Auskunftsverlangen nach Art. 15 DS-GVO nicht sichergestellt war. Des Weiteren wirkte sich negativ für das Unternehmen aus, dass es sich vorliegend nicht um einen Erstverstoß im Zusammenhang mit datenschutzrechtlichen Auskunftsverlangen handelte. Vielmehr wurde bereits aufgrund eines Verstoßes gegen § 43 Abs. 1 Nr. 8a BDSG a. F. i. V. m. § 34 Abs. 1 Satz 1 BDSG a.F. aus dem Jahr 2017 ein Ordnungswidrigkeitenverfahren gegen den damaligen und jetzigen Geschäftsführer des Unternehmens geführt und Mitte 2018 mit rechtskräftigem Urteil des Amtsgerichts Wiesbaden wegen einer fahrlässig, nicht vollständig erteilten Auskunft eine Geldbuße in Höhe von 1.000,00 Euro festgesetzt.

Damit die Geldbuße die von Art. 83 Abs. 1 DS-GVO intendierte Wirkung entfaltet, war die tatsächliche wirtschaftliche Fähigkeit des Unternehmens mit einzubeziehen. Aufgrund der Angaben im Jahresabschluss des Unternehmens ging ich davon aus, dass die ausgesprochene Gesamtgeldbuße die Leistungsfähigkeit des Unternehmens nicht übersteigt und für diese auch keine unverhältnismäßige Belastung darstellt. Nach Abwägung aller für und gegen die verantwortliche Stelle sprechenden Kriterien liegt die Geldbuße weit im unteren Bereich des Bußgeldrahmens. Das Verfahren ist noch nicht rechtskräftig abgeschlossen.

16.2
Zwischen Maßnahmen und Sanktionen – Entwicklung der Umsetzung des Art. 58 Abs. 2 DS-GVO in der Praxis

Art. 57 Abs. 1 lit. u DS-GVO verpflichtet den HBDI, interne Verzeichnisse nach Art. 58 Abs. 2 DS-GVO zu führen. Die Bilanz zeigt, dass sich das Zusammenspiel zwischen Maßnahmen und Sanktionen positiv entwickelt hat.

Nach Art. 57 Abs. 1 lit. u DS-GVO bin ich verpflichtet, interne Verzeichnisse über Verstöße gegen die DS-GVO und gemäß Art. 58 Absatz 2 DS-GVO ergriffene Maßnahmen auf meinem Hoheitsgebiet, also in meinem Zustän-

digkeitsbereich, zu erstellen. Bis Ende 2020 habe ich im Berichtsjahr 31 Verwarnungen nach Art. 58 Abs. 2 lit. b DS-GVO ausgesprochen; ich habe eine Anweisung nach Art. 58 Abs. 2 lit. c DS-GVO an den Verantwortlichen oder Auftragsverarbeiter, den Anträgen der betroffenen Person auf Ausübung der ihr nach der DS-GVO zustehenden Rechte zu entsprechen, erteilt; ich habe acht Anweisungen nach Art. 58 Abs. 2 lit. d DS-GVO, die Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen, ausgesprochen; darüber hinaus habe ich vier Maßnahmen nach Art. 58 Abs. 2 lit. f DS-GVO, nach denen eine vorübergehende oder endgültige Beschränkung einschließlich eines Verbots ausgesprochen wurde, erteilt sowie zwei Bußgeldbescheide nach Art. 58 Abs. 2 lit. i i. V. m. Art. 83 DS-GVO verhängt, s. a. Abb. Teil I Ziff. 17.2.

Entwicklung der Abhilfebefugnisse nach Art. 58 Abs. 2 DS-GVO

Für die Aufsichtspraxis und auch für die Verantwortlichen und Auftragsverarbeiter war das Abhilfeinstrumentarium nach Art. 58 Abs. 2 DS-GVO in den ersten zwei Jahren noch Neuland. Die Entwicklung im Berichtsjahr zeigt deutlich, dass langsam eine Routine in der Anwendung der zur Verfügung stehenden breiten Maßnahmenpalette nach Art. 58 Abs. 2 DS-GVO eintritt.

Art. 58 Abs. 2 DS-GVO

Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen diese Verordnung verstoßen,

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,

c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen,

d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen,

f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,

g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,

h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,

i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,

j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.

Die Konzeption des Art. 58 Abs. 2 DS-GVO ist für die Aufsichtspraxis ein großer Gewinn, um die Einhaltung der Normen der DS-GVO sicherzustellen. Aus der Konzeption der Norm wird deutlich, dass der Aufsichtsbehörde nicht nur Bußgelder zur Verfügung stehen, um auf Verstöße gegen die DS-GVO zu reagieren. Die Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO sind im Gesamtpaket das, was die scharfe Klinge des Schwertes der Aufsicht ausmacht.

Neben der Möglichkeit der Warnung nach Art. 58 Abs. 2 lit. a DS-GVO, die der Aufsichtsbehörde die Option einräumt, präventiv gegen einen Verstoß vorzugehen, greifen die Abhilfemaßnahmen nach Art. 58 Abs. 2 lit. b bis j DS-GVO dann, wenn ein Verstoß festgestellt wurde.

Die Abhilfebefugnisse nach Art. 58 Abs. 2 lit. b – j lassen sich wiederum aufteilen in Sanktionen und Maßnahmen.

Im Vordergrund des aufsichtsbehördlichen Handelns steht das Abstellen des Verstoßes. Es folgt in der Regel dann die Prüfung, ob es einer Sanktion bedarf, und die Entscheidung darüber, welche Sanktion im konkreten Einzelfall zur Anwendung kommen soll. In Ausnahmefällen kann diese auch schon zu einem früheren Zeitpunkt erfolgen.

Maßnahmen

Die Maßnahmen nach Art. 58 Abs. 2 lit. c-h und j DS-GVO lassen sich strukturieren. Sie lassen eine Systematik erkennen, die Eskalationsstufen aufweist.

Die Anweisung nach Art. 58 Abs. 2 lit c DS-GVO bezieht sich konkret auf die im Kontext mit den Betroffenenrechten gestellten Anträge. Wenn beispielsweise auf einen Antrag nach Art. 15 DS-GVO zu Unrecht die Auskunft verweigert wird, dann kann ich die verantwortliche Stelle anweisen, dieses Anliegen zu erfüllen. Wird die Anweisung nicht erfüllt, habe ich die Möglichkeit, den Bescheid mit Verwaltungszwangsmaßnahmen zu verbinden.

Mit Art. 58 Abs. 2 lit. d DS-GVO eröffnet mir die Verordnung die Möglichkeit, eine Anweisung gegenüber Verantwortlichen oder Auftragsverarbeitern zu

erlassen und diese anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen. Sollte diese Maßnahme nicht zum Erfolg führen, gibt es hierzu eine Eskalationsstufe. Denn dann sind Maßnahmen nach Art. 58 Abs. 2 lit. f DS-GVO unter Umständen geeignet, einen datenschutzkonformen Zustand zu erreichen. Dann ist eine Situation gegeben, die es ggf. rechtfertigen würde, die Verarbeitung vorübergehend oder unter Umständen sogar endgültig zu beschränken oder gar ein Verbot der Verarbeitung auszusprechen. Dies ist im jeweiligen Einzelfall zu prüfen.

Maßnahmen nach den Buchstaben g, h, j musste ich bislang nicht aussprechen. Art. 58 Abs. 2 lit. g DS-GVO räumt mir das Recht ein, die Berichtigung oder Löschung von personenbezogenen Daten oder die Beschränkung der Verarbeitung gemäß den Art. 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Art. 17 Abs. 2 und Art. 19 offengelegt wurden, über solche Maßnahmen zu unterrichten. Das wäre im Grunde die Eskalationsstufe zu einer Maßnahme nach Art. 58 Abs. 2 lit. c DS-GVO. Art. 58 Abs. 2 lit. h DS-GVO wird in der Praxis eine Rolle spielen, wenn die Zertifizierung nach Art. 42 und 43 DS-GVO mit Leben gefüllt wird. Bislang wurden noch keinen Genehmigungen erteilt. Nach Art. 58 Abs. 2 lit. j DS-GVO dürfte ich die Aussetzung der Übermittlung von Daten an einen Empfänger in ein Drittland oder eine internationale Organisation anordnen. Aber auch hiervon habe ich im Berichtsjahr keinen Gebrauch gemacht.

Sanktionen

Zusätzlich oder an Stelle der geeigneten Maßnahmen, die gemäß dieser Verordnung verhängt wurden, sollte die Aufsichtsbehörde Sanktionen einschließlich Geldbußen verhängen (s. Erwägungsgrund 148 DS-GVO). Im Fall eines geringfügigeren Verstoßes oder falls die voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, kann anstelle einer Geldbuße eine Verwarnung erteilt werden. Die in Erwägungsgrund 148 angesprochenen Sanktionen finden sich zwischen den Abhilfebefugnissen in Art. 58 Abs. 2 unter lit. b und i DS-GVO wieder.

Über das Bußgeldverfahren habe ich bereits in meinem 47. und 48. Tätigkeitsbericht berichtet. Das Bußgeldverfahren ist die Ultima ratio. Bei geringfügigen Verstößen habe ich im Berichtsjahr von der Möglichkeit des Ausspruchs einer Verwarnung Gebrauch gemacht. Dem lag immer eine Abwägung über die geeigneten, erforderlichen und verhältnismäßigen Mittel zugrunde.

Im Berichtsjahr wurden im Vergleich zum Vorjahr knapp doppelt so viele Verwarnungen ausgesprochen. Die Besonderheit dieser Verwarnung ist,

dass sie ohne ein Verwarngeld ausgesprochen wird. Das Verfahren über die Verwarnung richtet sich nach dem Hessischen Verwaltungsverfahrensgesetz und nicht nach den Vorschriften des Ordnungwidrigkeitengesetzes. Bei meiner Entscheidung über die Art der Sanktion habe ich die Anforderungen aus Erwägungsgrund 148 S. 3, die sich mit den Kriterien nach Art. 83 Abs. 2 DS-GVO weitestgehend decken, berücksichtigt und diese in meine Entscheidung über die Art der Sanktion einfließen lassen.

16.3
Entwicklung der Verwaltungsgerichtsverfahren beim HBDI

Seit dem Inkrafttreten der DS-GVO im Mai 2018 hat die Zahl der Verwaltungsgerichtsverfahren stark zugenommen. Die Betroffenen wandten sich im Bereich der Auskunfteien gegen die Abschlussentscheidung im Aufsichtsverfahren, im Bereich der Videoüberwachung und des Beschäftigtendatenschutzes wurden die erlassenen Maßnahmen nach Art. 58 Abs. 2 DS-GVO und aus dem Bereich des Beschäftigtendatenschutzes die Feststellung von Verstößen angegriffen.

Seit Beginn 2019 verzeichne ich eine deutliche Zunahme der Klageverfahren gegen meine Aufsichtsentscheidungen vor dem Verwaltungsgericht. Mit der europäischen Datenschutzreform wurde in Art. 78 Abs. 1 DS-GVO das Recht auf wirksamen Rechtsbehelf gegen eine Aufsichtsbehörde gestärkt und das vor dem 25. Mai 2018 eher formlose Handeln hat sich in ein verwaltungsförmliches Handeln verwandelt.

Art 78 Abs. 1 DS-GVO

Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

Betroffene und Gerichtsverfahren

Betroffene, die Beschwerde bei mir einreichen, sind nach Art. 77 Abs. 2 DS-GVO durch mich über den Stand und die Ergebnisse der Beschwerde zu unterrichten sowie über die Möglichkeit des Rechtsbehelfs nach Art. 78 DS-GVO.

Art. 77 Abs. 2 DS-GVO

Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Artikel 78.

Betroffene können sich gemäß Art. 78 Abs. 1 DS-GVO i. V. m. § 20 BDSG gegen einen sie betreffenden rechtsverbindlichen Beschluss wenden. Darüber hinaus kann die betroffene Person sich gem. Art. 78 Abs. 2 DS-GVO mit einem wirksamen Rechtsbehelf gegen mich wenden, wenn ich mich nicht mit einer Beschwerde befasse oder sie nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der gemäß Art. 77 DS-GVO erhobenen Beschwerde in Kenntnis setze.

Verantwortliche, Auftragsverarbeiter und Gerichtsverfahren

Verantwortliche und Auftragsverarbeiter können sich gem. Art. 78 Abs. 1 i. V. m. § 20 BDSG und der VwGO gegen meine Maßnahmen nach § 58 Abs. 1, 2 und 3 DS-GVO wenden. Ausgenommen sind die Bußgeldverfahren, die gem. § 41 BDSG sich nach dem OWiG, der StPO und dem GVG richten.

Zuständiges Verwaltungsgericht

Örtlich zuständig für Klagen gegen meine Verwaltungsentscheidungen ist gemäß § 20 Abs. 3 BDSG das Verwaltungsgericht Wiesbaden und in zweiter Instanz der Verwaltungsgerichtshof in Kassel.

Zur Statistik

Seit Beginn 2019 sind 46 Verwaltungsgerichtsverfahren über Datenschutzfragen rechtshängig geworden. Ende 2020 hatte ich noch 24 Verfahren vor dem Verwaltungsgericht Wiesbaden offen (Teil I Ziff. 17.2.).

Die Gerichtsverfahren werden von meiner Behörde selbst, durch das Justiziariat, geführt, das auch für die Durchführung der Bußgeldverfahren zuständig ist.

Schwerpunkte der Verwaltungsgerichtsverfahren waren Fragen aus den Fachbereichen Auskunfteien, Beschäftigtendatenschutz, Videoüberwachung und Auskunftsrechte nach Art. 15 DS-GVO.

Die überwiegende Zahl der Verwaltungsgerichtsverfahren richtete sich gegen Bescheide, die der Beschwerde führenden Person i. S. d. Art. 77 Abs. 2 DS-GVO eröffneten, dass nach Prüfung der Beschwerde festgestellt worden sei, dass kein Verstoß vorliegt. Bei den beiden Klagen wegen Untätigkeit

nach Art. 78 Abs. 2 DS-GVO stellte sich im Ergebnis heraus, dass diese unbegründet waren.

Die beiden Verfahren wegen Videoüberwachung aus den Jahren 2019 und 2020 wurden in 2020 erfolgreich abgeschlossen. Die Klage gegen die angeordneten Maßnahmen zur Herstellung einer datenschutzkonformen Videoüberwachung konnte durch die Einsicht der Klägerpartei nach einem vom Gericht anberaumten Ortstermin mittels Erledigung nach § 161 VwGO erfolgreich abgeschlossen werden.

Offengeblieben ist bislang, ob der feststellende Verwaltungsakt, der einen Verstoß gegen die DS-GVO ohne den Ausspruch einer Verwarnung als ein Minus zur Verwarnung nach Art. 58 Abs. 2 DS-GVO feststellt, ein rechtmäßiger Verfahrensabschluss ist. Derzeit wird vertreten, dass man einen solchen Bescheid als ein Minus zur Verwarnung auf Art. 58 Abs. 2 lit. b DS-GVO stützen kann.

Die Verwaltungsgerichtsverfahren wurden überwiegend mittels Klagerücknahme nach § 92 VwGO oder Erledigung oder unter Abschluss eines Vergleichs beendet.

17. Arbeitsstatistik Datenschutz

17.1 Zahlen und Fakten

Die statistische Auswertung der Arbeitsmengen unter dieser Ziffer entspricht den formalen Anforderungen, die die Datenschutzkonferenz vorgibt, um eine bundeseinheitliche Aussage treffen zu können. Diese Werte werden u. a. der Europäischen Kommission und dem Europäischen Datenschutzausschuss gemäß Art. 59 DS-GVO vorgelegt.

Zahlen und Fakten	Fallzahlen 01.01.2020 bis 31.12.2020
a. „Beschwerden“	5.414
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).	(davon 855 Abgaben)
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.	1.983
c. „Meldungen von Datenschutzverletzungen“	
Anzahl schriftlicher Meldungen	1.433
d. „Abhilfemaßnahmen“	
Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.	
(1) nach Art. 58 Abs. 2 a (Warnungen)	(1) 1
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	(2) 31
(3) nach Art. 58 Abs. 2 c-g und j (Anweisungen und Anordnungen)	(3) 13
(4) nach Art. 58 Abs. 2 i (Geldbußen)	(4) 2
(5) nach Art. 58 Abs. 2 h (Widerruf von Zertifizierungen)	(5) 0
e. „Europäische Verfahren“	
(1) Anzahl der Verfahren mit Betroffenheit (Art.56)	(1) 198
(2) Anzahl der Verfahren mit Federführung (Art. 56)	(2) 5
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	(3) 724*

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 ggü. Gerichten.	54

*Im Vorjahr waren es noch **66** Verfahren.

17.2
Ergänzende Erläuterungen zu Zahlen und Fakten der Teil I Ziffer 17.1

Die nachstehenden Darstellungen erläutern und ergänzen die Auswertungen zu Teil I Ziff. 17.1 auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Insgesamt weisen die Zahlen eine deutliche Steigerung zum Vorjahr auf, das durch Eingaben im Kontext der neuen DS-GVO geprägt war. Auffällig im Jahr 2020 sind die Werte zu den Themenbereichen Auskunfteien und Inkassounternehmen, Schulen/Hochschulen, e-Kommunikation/Internet, Handel/Handwerk, Vereine/Verbände und Beschäftigtendatenschutz.

Beschwerden und Beratungen

Die datenschutzrechtliche Umsetzung der Vorgaben der Corona-Verordnungen durch die Verantwortlichen, Unsicherheiten von Arbeitgebern und Arbeitnehmern zu Home-Office-Fragen, die öffentliche Diskussion um Geschäftsmodelle von Auskunfteien und zu Produkten von Software-Herstellern waren Themen, die nahezu über das gesamte Jahr hinweg präsent waren.

Weiteren Beratungs- und Nachfragebedarf löste das sogenannte Schrems II-Urteil des EuGHs aus (Einzelheiten s. a. Beitrag Teil I Ziff. 2.2).

Neben den schriftlichen Eingaben wurde im Berichtsjahr besonders häufig der „schnelle“ Weg der Klärung durch telefonische Auskunft gesucht. Die Anliegen der Verantwortlichen und Betroffenen – aus dem öffentlichen und nichtöffentlichen Bereich – waren dringlich, wenn sie sich kurzfristig mit den Vorgaben der verschiedenen Corona-Verordnungen oder den Maßnahmen und Empfehlungen von Gesundheitsbehörden/RKI auseinandersetzen und auf sie reagieren mussten. Dies machte sich in dem enormen Anstieg der telefonischen Beratungen und Klärungen bemerkbar, die länger als zehn Minuten dauerten, aber letztlich keinen dokumentierten Niederschlag fanden.

Im Prüfbereich sei auf den Beginn der „neuen“ Prüftätigkeit nach § 29a HSOG bei zwei Polizeipräsidien hingewiesen.

Die nachfolgende Übersicht stellt die Mengen der Eingabe (Beschwerden und Beratungen) des Berichtsjahres im Vergleich zum Vorjahr dar:

Fachgebiete	Anzahl 2019			Anzahl 2020		
	Beschwerden	Beratungen	Eingaben insgesamt	Beschwerden	Beratungen	Eingaben insgesamt
Auskunfteien, Inkasso	923	19	**942**	1201	19	**1220**
Schule, Hochschule, Archive	56	312	**368**	191	545	**736**
e-Kommunikation, Internet	512	52	**564**	565	53	**618**
Beschäftigtendatenschutz	199	131	**330**	263	170	**433**
Videobeobachtung	253	95	**348**	317	90	**407**
Kreditwirtschaft	949	10	**959**	323	15	**338**
Handel, Handwerk, Gewerbe	182	58	**240**	264	74	**338**
Verkehr, Geodaten, Landwirtschaft	240	39	**279**	238	47	**285**
Gesundheit, Pflege	101	180	**281**	201	86	**287**
Betriebliche/ Behördliche DSB	16	219	**235**	17	258	**275**
Kommunen, Wahlen	115	112	**227**	137	115	**252**
Polizei, Justiz, Verfassungsschutz	129	32	**161**	201	73	**274**
Vereine, Verbände	57	77	**134**	80	119	**199**
Adresshandel, Werbung	174	6	**180**	169	4	**173**
Wohnen, Miete	54	66	**120**	65	59	**124**
Soziales	50	63	**113**	63	56	**119**
Versorgungsunternehmen	76	22	**98**	91	17	**108**
IT-Sicherheit, DV-Technik	30	57	**87**	3***	91***	**94**
Versicherungen	46	17	**63**	52	29	**81**
Rundfunk, Fernsehen, Presse	46	1	**47**	57	0	**57**
Religionsgemeinschaften				20	3	**23**
Datenschutz außerhalb der EU	3	6	**9**	11	29	**40**

Fachgebiete	Anzahl 2019			Anzahl 2020		
	Beschwerden	Beratungen	Eingaben insgesamt	Beschwerden	Beratungen	Eingaben insgesamt
Forschung, Statistik	10	1	**11**	10	1	**11**
Ausländerrecht	3	8	**11**	**s. Sonstiges**	**s. Sonstiges**	**s. Sonstiges**
Steuerwesen	1	0	**1**	**s. Sonstiges**	**s. Sonstiges**	**s. Sonstiges**
Sonstige Themen < 10 (z. B. Kammern, Ausländerwesen, Finanzwesen	33	27	**60**	20	6	**26**
Zwischensumme eschwerden und Beratungen	4.258	1.610	**5.868**	4.559	1.959	**6.518**
BCR-Verfahren mit deutscher oder europaweiter Federführung des HBDI			17			40
Meldungen von Datenpannen*			1.453			1433
Gesamtsumme dokumentierter Eingaben			**7.338**			**7.991**
Zzgl. Summe telefonischer Beratungen und Auskünfte von mehr als 10 Min.**			**7.044**			**9.444**
Gesamtsumme dokumentierter + telefonischer Eingaben			**14.382**			**17.435**

* siehe auch Beitrag Teil I Ziff. 15.1, 15.2

** Telefonische Nachfragen, die keinen schriftlichen Niederschlag finden, werden pauschaliert erfasst. Sie erfolgten als Beratungen, Auskünfte, Erläuterungen und Verständnisfragen zur DS-GVO u. Ä. sowohl zu allgemeinen Themen als auch zu spezifischen Fragestellungen, wie z. B. hinsichtlich des sog. Schrems II-Urteils des EuGH oder zur konkreten datenschutzrechtlichen Umsetzung der Corona-Verordnungen. Exemplarisch werden derartige Telefonate im November, als Monat ohne besondere Vorkommnisse, gezählt und als Durchschnittswert hochgerechnet.

*** Weitere IT-Themen waren begleitend zu einer rechtlichen Anfrage oder einer Datenpannenmeldung zu prüfen und wurden deshalb nicht eigenständig gezählt.

Weitere sonstige Aufgaben

Unberücksichtigt in den obigen Tabellen, aber nicht weniger erwähnenswerte Aufgaben und Themen, die im Berichtsjahr bearbeitet wurden, sind beispielsweise:

– **Tätigkeiten der internen Datenschutzbeauftragten beim HBDI**
Es wurden **35** Auskunftsersuchen von Bürgerinnen und Bürgern bzgl. der Verarbeitung ihrer Daten beim HBDI bearbeitet sowie **21** entsprechende Beratungen durchgeführt.

– **Regelmäßige Beratungen**
Mit den intern bestellten Datenschutzbeauftragten aus verschiedenen öffentlichen Bereichen (z. B. von Ministerien, Städten und Kommunen und den europäischen Datenschutz-Aufsichtsbehörden) wurden Austausche gepflegt und z. T. regelmäßige Beratungsleistungen erbracht.

– **Presse und Öffentlichkeitsarbeit**
Die Anzahl der Presseanfragen hat sich im Jahr 2020 mit **153** Anfragen gegenüber dem Jahr 2019 mit **49** Anfragen mehr als verdreifacht.

Zahlreiche Veröffentlichungen und Hilfestellungen wurden Verantwortlichen, Bürgern und Bürgerinnen auf der Homepage (z. B. im Gesundheitsbereich, für Vereine und Schulen) des HBDI zur Verfügung gestellt.

– **Ausbildungsleistungen**
Es wurden **vier** Referendare und Referendarinnen in ihren Wahl- bzw. Verwaltungsstationen ausgebildet.

– **Fortbildung und Vorträge**
Es wurden **15**, zum Teil mehrtägige datenschutzrechtliche Schulungen, Seminare und Fortbildungen im öffentlichen und nichtöffentlichen Bereich durchgeführt.

– **Teilnahme an Konferenzen, Arbeitskreisen und Arbeitsgruppen**
Beratungen und Abstimmungen der Aufsichtsbehörden untereinander und in ihren Gremien auf Landes-, Bundes- und EU-Ebene, aber auch übergreifend mit Ansprechpartnern aus außereuropäischen Drittstaaten, sind mittlerweile essenziell für einen erfolgreichen Datenschutz in Hessen. Die Gremienarbeit ist mitunter sehr zeitintensiv, aber nicht mehr verzichtbar. In den Zeiten der Corona-Lock-Downs wurden persönliche Treffen durch Videokonferenzen ersetzt. Die Konferenz der Datenschutz- und Informationsfreiheitsbeauftragten (DSK) tagte somit ca. alle zwei Monate zu aktuellen Themen. Die Ergebnisse des Jahres 2020 sind im Anhang I auszugsweise abgedruckt, im Einzelnen aber auch auf der Home-Page der Datenschutzkonferenz *www.datenschutzkonferenz.de* nachzulesen.

In den Arbeitskreisen der DSK ist der HBDI in allen Bereichen beteiligt. Auch in den Unterarbeitsgruppen, die zu Spezialthemen eingesetzt werden, engagieren sich Mitarbeiterinnen und Mitarbeiter des HBDI. In zahlreiche EU-Gremien (z. B. BTLE, CSC, SCG SIS II, SCG Eurodac, SCG VIS) konnte HBDI seine Mitarbeit einbringen. Daneben erfolgten auch Unterstützungsleistungen an die EU-Kommission wie z. B. durch die Teilnahme und Beiträge im Rahmen der Schengen-Evaluierung.

Abhilfemaßnahmen und Gerichtsverfahren (s. a. Beiträge Teil I Ziff. 16.2, 16.3)

Abhilfemaßnahmen	Anzahl
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	1
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	31
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	13
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	2
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0
Gesamt	**47**

Gerichtsverfahren	Anzahl
Klagen gemäß Art. 78 Abs. 1 DS-GVO	19
Klagen gemäß Art. 78 Abs. 2 DS-GVO	2
Sonstige	4
Gesamt	**25**

Meldungen von Datenschutzverletzungen

a. Meldungen nach Art. 33 DS-GVO und § 60 HDSIG (s. a. Beitrag Teil I Ziff. 15.1, 15.2)

Gesamtübersicht	
Grund	**Anzahl**
– Fehlversand	494
– Hackerangriffe, Phishing, Schadsoftware	184
– Verlust/Diebstahl von Unterlagen, Datenträgern etc.	142
– Unrechtmäßige Offenlegung/Weitergabe von Daten	107
– Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	85
– Offener E-Mail-Verteiler	76

– Missbrauch von Zugriffsrechten	43
– Unzulässige Veröffentlichung	25
– Fehlerhafte Zuordnung von Daten	21
– Nicht datenschutzkonforme Entsorgung	9
– Unverschlüsselter E-Mail-Versand	7
– Sonstige	240
Gesamt	**1.433**

am stärksten betroffene Bereiche	
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	491 Fälle
Beschäftigtendatenschutz	254 Fälle
Gesundheitsbereich	230 Fälle

Anhang zu I

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

1.1
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 25.11.2020

Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten

Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicherheitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.

Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs- und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021 nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht

auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vgl. BVerfG, o. g. Beschluss vom 27. Mai 2020, Rn. 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.

1.2
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 25.11.2020

Betreiber von Webseiten benötigen Rechtssicherheit Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen

Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie[1] vollständig und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) umzusetzen.

Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt hat.[2] Das Urteil des Bundesgerichtshofs (BGH)

1 Richtlinie 2002/58/EG in der letzten Änderung durch die Richtlinie 2009/136/EU

2 Siehe Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015, abrufbar unter: *https://www.datenschutzkonferenzonline.de/media/en/20150205_en_Entschliessung_Cookies.pdf*

vom 28. Mai 2020 (I ZR 7/16 – „Planet49“) verstärkt nach Auffassung der DSK den seit langem bestehenden dringenden Handlungsbedarf.

Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018“ den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der DSGVO nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.[3]

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Abs. 3 Telemediengesetz (TMG) wäre ein solches Vorgehen dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 ePrivacy-Richtlinie legt der BGH § 15 Abs. 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der BGH der Vorabentscheidung des Europäischen Gerichtshofes gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.

Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacy-Richtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene

3 Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“, abrufbar unter: *https://www.datenschutzkonferenz-online.de/anwendungshinweise.html*), Orientierungshilfe für Anbieter von Telemedien (*https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf*).

weitgehend abschließend durch die Datenschutz-Grundverordnung geregelt. Art. 5 Abs. 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Abs. 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.

§ 15 Abs. 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Abs. 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste u. a. in Bezug auf „Cookies“ rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen.

1.3
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 25.11.2020

Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf „Si-

cherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist essenzielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integere Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangsgesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das „Schrems II“-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten.

Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.

Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Art. 7 GRCh geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Art. 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Art. 10 GG und ergänzend durch das Recht auf

informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.

Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integerer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integerer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integere Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

1.4
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020

Datenschutz braucht Landgerichte auch erstinstanzlich

Mit dem *„Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens“* (BR-Drs. 107/20 (B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen nach der Datenschutz-Grundverordnung (DSGVO) über 100.000 Euro streichen. Selbst über Geldbußen in dieser Höhe sollen künftig die Amtsgerichte entscheiden.

Das Ziel der Effektivierung des Bußgeldverfahrens wird mit dem geplanten Gesetz jedoch nicht erreicht werden. Der Gesetzentwurf verkennt in eklatanter Weise die besondere wirtschaftliche, technische und rechtliche Komplexität von DSGVO-Geldbußen. Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte zudem nicht etwa entlasten, sondern noch stärker als bisher belasten.

Das Sanktionsrecht der DSGVO ist – anders als der Bundesrat unterstellt – mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Datenschutz-Ordnungswidrigkeiten mit Geldbußen über 100.000 Euro weisen wirtschaftlich und technisch eine besondere Komplexität auf und bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind viel eher mit Wirtschaftsstrafsachen vergleichbar, die ohnehin den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DSGVO am Kartellrecht orientiert. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Abs. 2 Satz 1 Bundesdatenschutzgesetzes (BDSG) zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der Strafkammern als sog. große Bußgeldkammern entsprechend § 76 GVG vorsieht.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert daher die Beibehaltung der landgerichtlichen Zuständigkeit für DSGVO-Geldbußen über 100.000 Euro und warnt vor einer Streichung der Vorschrift und deren Folgen.

1.5
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020

Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[1] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

1 Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter *https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver-%C3%A4nit%C3%A4t*

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[2] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten“. Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist, und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sicher-

2 PwC Strategy & (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter *https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile*

gestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

– die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,
– bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und
– die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:
   – Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.
   – Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.
   – Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.
2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:
   – Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.
3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

- Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:
   - Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.
   - Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).
5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:
   - Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung

hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

1.6
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 01.09.2020

Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen.

Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden.

Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der EPA, d. h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte

(Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d. h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs. 164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

1.7
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 26.08.2020

Registermodernisierung verfassungskonform umsetzen!

Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz – RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll u. a. eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.

Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12.09.2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.

Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen von jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potenzial der möglichen missbräuchlichen Verwendung.

So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte

Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks. Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.

Die Datenschutzkonferenz hatte demgegenüber „sektorspezifische" Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.

Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf „rechtliche, technische und organisatorische Komplexität" abgelehnt.

Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den „Eilbedarf" unter den Tisch fallen zu lassen.

Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

1.8
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 16.04.2020

Polizei 2020 – Risiken sehen, Chancen nutzen!

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten „fachlichen Bebauungsplan" für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des

Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

1. Umfassende Bestandsaufnahme

Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken

Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerte- und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste“ zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung“, ein „Basisdienst Datenqualität“ und ein „Basisdienst Aufsicht und Kontrolle“.

1.9
Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 03.04.2020

Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

– Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat.

Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

– Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.
– Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder – wie eine vorherige Anonymisierung – sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.
– Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.
– Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. **Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des

Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

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 – 26.11.2020

Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise

In der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde ein Prüfschema zum datenschutzkonformen Einsatz von Windows 10 beschlossen und anschließend veröffentlicht.[1] Damit soll den Verantwortlichen die Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Einsatz von Windows 10 erleichtert werden. Eine Arbeitsgruppe der DSK hat unter Beteiligung von LDA Bayern, BfDI, LfDI Mecklenburg-Vorpommern und LfD Niedersachsen seitdem ihre Untersuchung von Windows 10 in Hinblick auf die Telemetriestufe Security, die in der Enterprise-Edition verfügbar ist, fortgesetzt.

Unabhängig davon hat sich das an einer Laboruntersuchung der Arbeitsgruppe neben dem LfD Bayern als Gast beteiligte BSI selbst in einer umfangreichen Studie (SiSyPHuS-Studie) auch mit Fragestellungen der Windows-10-Telemetriefunktion beschäftigt.

Untersuchungsergebnisse der DSK-Arbeitsgruppe

Die Arbeitsgruppe hat die Telemetrie von Windows 10 einer Laboruntersuchung unterzogen, um festzustellen, ob sich die Telemetriedatenübermittlung durch Konfiguration unterbinden lässt. Microsoft hat gegenüber den Aufsichtsbehörden erklärt, dass bei der Nutzung der Telemetriestufe Security keine Telemetriedaten[2] übermittelt werden.

Es wurde Windows 10 Enterprise in der Version 1909 in drei Testszenarien untersucht. In allen drei Szenarien wurden Benutzeraktivitäten simuliert, um realistische Ergebnisse zu erzielen.

---

1 *https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf*

2 Zum Begriff siehe Bericht Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion (Anlage 1)

1. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum
2. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Basic“, 30 Minuten Testzeitraum
3. Keine Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

Die Details der Untersuchung können dem Laborbericht (Anlage 1) entnommen werden.

Die Untersuchung hat bestätigt, dass im zweiten Prüfszenario die Übermittlung von Telemetriedaten festgestellt werden konnte. Im dritten Szenario wurde ein Verbindungsaufruf zum settings-win.data.microsoft.com Endpunkt festgestellt. Dieser Endpunkt wird laut Aussage von Microsoft von mehreren Windows-10-Systemkomponenten, auch von der Telemetriekomponente, angesteuert. Nutzt die Telemetriekomponente diesen Endpunkt, besteht die Möglichkeit, dass hierüber Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten. Microsoft hat diesen Aufruf gegenüber den Datenschutzaufsichtsbehörden auf Basis eines Microsoft zur Verfügung gestellten Laborszenarios erläutert und erklärt diesen mit einer anderen Systemkomponente abseits der Telemetrie. Microsoft hat auf mündliche Nachfrage gegenüber den Datenschutzaufsichtsbehörden erklärt, dass trotz eines – möglicherweise aufgrund eines Softwarefehlers – unbeabsichtigten Aufrufs an den settings-win.data.microsoft.com Endpunkt von dem Telemetriedienst bei einem Telemetrielevel „Security“ weiterhin keine Telemetriedatenübermittlung stattfinden würde.

Untersuchungsergebnisse des BSI

In einer den Labortest der Arbeitsgruppe ergänzenden Untersuchung des Windows-10-Enterprise-Datenverkehrs durch das BSI im Januar 2020 wurden Datenübertragungen zu „settings-win.data.microsoft.com“ festgestellt (siehe Anlage 2).

Dabei wurden ein Windows 10 Enterprise System Version 1803 mit Telemetrielevel Security und „Windows Restricted Traffic Limited Functionality Baseline“ genutzt. Es ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com“ nicht im Klartext analysiert werden konnten und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt. Vor diesem Hintergrund hält das BSI aufgrund eines Defense-in-Depth-Ansatzes zur Stärkung der Sicherheit der IT-Systeme des Bundes an der Notwendigkeit

einer Netztrennung von Windows-10-Clients der Bundesverwaltung, auch zur Abwehr von Schadcodes, fest.

Laut Microsoft wird über den Endpunkt „settings-win.data.microsoft.com“ auch die Konfiguration der Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ dynamisch aktualisiert.[3] Auch im BSI-Projekt „SiSyPHuS“ ist diese Adresse mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt.[4]

Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne dass der Nutzer dem zustimmen müsse oder das kontrollieren könne. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt nach der Bewertung des BSI zumindest als bedenklich einzustufen.

Konsequenzen für Verantwortliche

Im veröffentlichten Prüfschema wird erläutert, dass Verantwortliche den Nachweis für die Rechtmäßigkeit etwaiger Übermittlungen personenbezogener Daten an Microsoft erbringen oder die Übermittlung personenbezogener Daten unterbinden müssen.

Zur Unterbindung der Übermittlung personenbezogener Telemetriedaten haben die Verantwortlichen beim Einsatz der Enterprise-Edition die Telemetriestufe Security zu nutzen und mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherzustellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.

Angesichts ggf. weiterer offener Fragen, die z. B. mit dem Aufruf der „settings-win.data.microsoft.com“-Datenverbindung verbunden sind oder die auch die SiSyPHuS-Studie des BSI aufwirft, wie des Umstands, dass die vorliegenden Untersuchungen auf Grund laufender Fortentwicklungen der Software natürlich nur eine Momentaufnahme darstellen, können die bisherigen Untersuchungen Verantwortliche nicht abschließend von ihrer aus Art. 5 Abs. 2 DS-GVO abzuleitenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst recht für Verantwortliche, die

3 *https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints*

4 *https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf*

Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.

Deshalb sollte Windows 10 in allen angebotenen Editionen die Möglichkeit bieten, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den in den Laboruntersuchungen der DSK und der SiSyPHus-Studie des BSI aufgezeigten verbliebenen Unwägbarkeiten werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

Die Landesbeauftragte für den Datenschutz Niedersachsen

Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion

Verantwortliche Durchführung für Tests und Dokumentation:	LfD Niedersachsen, Referat 3 - IT-Labor
Abschlussdatum der Tests:	14.05.2020
Finalisierung und Freigabe der Dokumentation:	17.06.2020

1 Zielsetzung des Tests

Microsoft gibt an, dass keine Übermittlung von Telemetriedaten an Microsoft erfolgt, wenn das Betriebssystem Windows 10 Enterprise sowie das von Microsoft zur Verfügung gestellte „Windows Restricted Traffic Limited Functionality Baseline“ (V1903)[1] installiert wurde.

Ende letzten Jahres wurde bereits ein Telemetrie-Test ohne Nutzerinteraktion am Windows 10 Enterprise System (durch die *Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen)* und das *Bayerische Landesamt für Datenschutz Aufsicht (BayLDA)*) durchgeführt.

Bei diesem Test wurde festgestellt, dass die datenschutzrechtlich kontrovers diskutierten Telemetriedaten bei Einsatz der Enterprise Version im überprüften Szenario deaktivierbar sind.[2]

Da Telemetriedaten ggf. erst bei Nutzeraktivität übertragen werden, soll dieser Aspekt nun in dem vorliegenden Test berücksichtigt werden.

Dazu werden die auftretenden Datenübertragungen protokolliert (Wireshark[3]-Protokolle).

Anschließend wird untersucht, ob sich in den Protokollen Verbindungen an die von Microsoft angegebenen Endpunkte („Telemetrie-Verbindungen“) finden.

Diese Endpunkte werden von Microsoft wie folgt angegeben[4]:

[1] Windows Restricted Traffic Limited Functionality Baseline: https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services, downloadlink: https://go.microsoft.com/fwlink/?linkid=828887, herunter geladen am 8.1.2020
[2] Siehe 9. Tätigkeitsbericht des BayLDA 2019: https://www.lda.bayern.de/media/baylda_report_09.pdf, Seite 22
[3] https://www.wireshark.org/
[4] https://docs.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization

Windows-Version	Endpunkt
Windows 10, Version 1703 oder höher, mit installiertem kumulativen Update 2018-09	**Diagnosedaten:** v10c.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1803 oder höher, ohne kumulatives 2018-09-Update installiert	**Diagnosedaten:** v10.events.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com
Windows 10, Version 1709 oder früher	**Diagnosedaten:** v10.vortex-win.data.microsoft.com
	Funktional: v20.vortex-win.data.microsoft.com
	Microsoft Defender Advanced Threat Protection ist länderspezifisch; das Präfix ändert sich je nach Land,
	z.B.: **de**.vortex-win.data.microsoft.com
	Einstellungen: settings-win.data.microsoft.com

Verbindungen zu anderen Microsoft-Diensten, wie z. B. Windows Update Diensten, Windows Aktivierungsdiensten oder Zertifikatsdiensten können ebenfalls im Wireshark Protokoll auftauchen, stellen aber keine „Telemetrie-Verbindungen“ im Sinne der Definition dieses Tests dar.

Es gilt somit, herauszufinden, ob im Wireshark Protokoll Verbindungen zu den in der Tabelle auf-gelisteten Microsoft Endpunkten auftauchen.

Der Test beinhaltet drei unterschiedliche Prüfszenarien:

Prüfszenario 1 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 0):

- Installation des „Windows Restricted Traffic Limited Functionality Baseline". Dadurch wird u.a. der Telemetrielevel des Systems auf „0" gesetzt.
- 72 Stunden Betrieb eines Windows 10 Enterprise Systems, mit installiertem Microsoft „Windows Restricted Traffic Limited Functionality Baseline" (V1903) und verschiedenen, teilweise automatisiert ablaufenden, Benutzeraktivitäten (mit systemnahen Programmen, jeweils nach Zeitplan) innerhalb der 72 Stunden des Tests.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

Prüfszenario 2 (Windows Restricted Traffic Limited Functionality Baseline, Telemetrielevel = 1):
Laut Aussage von Microsoft ist für die tatsächliche Unterbindung der Telemetriedaten-Übermittlung das Setzen des Telemetrielevels auf „0" ausreichend.

Mit dem Prüfszenario 2 soll überprüft werden, ob bei einem Telemetrielevel größer als „0" Netzwerkverbindungen zu den von Microsoft benannten Endpunkten in den Protokollen zu finden sind.

Der Telemetrielevel kann durch folgende Registry-Einträge geändert werden:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection`
- `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\DataCollection`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`

Der dort jeweils wiederzufindende Parameter *„AllowTelemetry"* bzw. *„Value"*
(in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\default\System\AllowTelemetry`)
stellt mit den möglichen Werten 0-3 die Intensität der Microsoft-seitigen Telemetriedaten-Übermittlung dar:

- 0 = „security" = Keine Telemetriedaten Erfassung und Übermittlung bis
- 3 = „full" = Vollständige Telemetriedaten Erfassung und Übermittlung

Anmerkung: der Telemetrielevel „0" kann in den Windows Home und Pro-Versionen von Windows 10 nicht gesetzt werden.

Der Versuchsaufbau in Prüfszenario 2 wird zum Prüfszenario 1 daher nur in einem Punkt (ceteris paribus) wie folgt abgeändert:

- Der Parameter-Wert *„AllowTelemetry“* (bzw. „Value“) wird manuell in den dazu verfügbaren Registrierungsvariablen auf „1“ (= „einfach“ bzw. „basic“) gesetzt.
- Laufzeit des Tests: 30 Minuten.
    - Die verkürzte Laufzeit ist damit begründet, dass zu erwarten ist, dass in Telemetrielevel 1 bereits nach kurzer Zeit Verbindungen zu den in der o.g. Tabelle angegebenen Endpunkten (insbesondere zu *v10.events.data.microsoft.com*) stattfinden.
    - Folgende Benutzeraktivitäten am Windows 10 System werden in den 30 Testminuten durchgeführt:
        - Einstecken eines beliebigen USB Sticks.
        - Erstellen einer Notepad Datei.
        - Abspeichern der Datei auf dem USB Stick.
        - Manuelles Starten des Browsers und Aufruf der Website www.rki.de mit anschließendem Aufruf von drei Links derselben Website.
        - Schließen des Browsers.
        - Start des *Invoke User Simulators* (automatisiertes Webbrowsen).

Prüfszenario 3 (Standard-Windows-Installation, Telemetrielevel = 0):
Das in Prüfszenario 1 und 2 installierte Microsoft „Windows Restricted Traffic Limited Functionality Baseline“ unterbindet nicht nur den Telemetrie-Verkehr. Es werden auch viele von Microsoft standardmäßig installierte „Zusatzprodukte“ deinstalliert. Dadurch werden die Netzwerkverbindungen an Microsoftsysteme deutlich reduziert.
In manchen Fällen möchte ein Verantwortlicher aber diese „Zusatzfunktionalitäten“ nutzen.

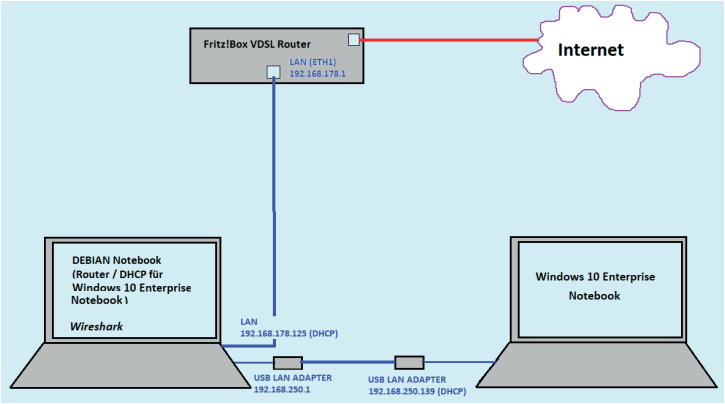
Für den Verantwortlichen wäre es also relevant zu wissen, ob die Unterbindung der Telemetrie-Datenübermittlung nur durch Setzen des Telemetrielevels auf „0“ möglich ist, ohne das „Windows Restricted Traffic Limited Functionality Baseline“ zu installieren und somit andere (ggf. im Unternehmensumfeld benötigte) Microsoft Dienste zu nutzen, die durch die Installation des Paketes nicht zur Verfügung stehen würden.

Um dies zu prüfen, wird folgender Test durchgeführt:

- Standard Installation von Windows 10 Enterprise.
- Manuelles Setzen des Telemetrielevel des Systems auf „0“.
- 72 Stunden Benutzeraktivitäten am Windows 10 System, nach Zeitplan.
- Mitschnitt des dabei aufgetretenen Netzwerkverkehrs.
- Auswertung des Wireshark Protokolls auf Vorhandensein von Verbindungen zu relevanten Microsoft Endpunkten (s.o.).

2 Beschreibung des Laboraufbaus

2.1 Grafische Darstellung des Laboraufbaus



2.2 Folgende Hardware Komponenten und Konfigurationen werden verwendet:

2.2.1 Notebook Lenovo Typ 20KE-S9020

Konfiguration:

- Windows 10 Enterprise V1909.
  Workgroup Installation ohne Anbindung an eine Domäne.
- Alle zum Testzeitpunkt vorhandenen Microsoft Updates werden installiert.
- Microsoft „ Windows Restricted Traffic Limited Functionality Baseline" (V1903) wird installiert (Prüfszenario 1 und 2).
- Kommandozeile: *ipconfig /flushdns* wird vor Durchführung jedes Prüfszenarios ausgeführt.
- Es werden darüber hinaus keine weiteren Veränderungen am Windows 10 Enterprise System vorgenommen.
- Das System wird vor jedem Test neu gestartet.

2.2.2 Notebook Fujitsu Typ E734 mit Betriebssystem Debian 10

Konfiguration:

- Nutzung der integrierten ETH NW Schnittstelle als Verbindung zur Fritz!Box.
- IP Adresse (192.168.178.x Bereich) wird per DHCP von der Fritz!Box an das Debian Notebook verteilt.
- Eine zusätzlich angeschlossene USB Netzwerkkarte dient als Netzwerk- Schnittstelle zum Windows 10 Enterprise Notebook.

- Das Debian Notebook fungiert als Router durch Nutzung des LINUX Dienstes *dnsmasq* für das Windows 10 Enterprise Testnotebook.
- DHCP Router Dienst läuft auf Debian Notebook und vergibt IP (im Adressbereich 192.168.250.x) an das Windows 10 Enterprise Notebook.

2.2.3 Fritz!Box 7590

- Dient als Netzwerk-Router für das Debian Notebook mit V-DSL Verbindung zum Internet.
- Vor jedem Prüfszenario wird der DNS Cache der Fritz!Box geleert.

3 Beschreibung des Testablaufs

Der Test simuliert einen 72 stündigen Betrieb des Windows 10 Enterprise Notebooks.
Es werden in unterschiedlichen Zeitabständen (die minutengenau in einer Tabelle erfasst sind), am Windows 10 Enterprise Notebook manuelle Tätigkeiten mit unterschiedlichen Softwarekomponenten sowie durch ein Skript gesteuerte Browseraktivitäten vorgenommen, um Anwendertätigkeiten zu simulieren.

Dazu wird eine Teilkomponente eines automatisch ablaufenden Power-Shell Skripts verwendet. Das Skript mit dem Namen *„Invoke-UserSimulator“* wurde zur automatisierten Simulation von auf dem PC ablaufenden Vorgängen entwickelt. Es ist über *Github*[5] frei verfügbar.
Verwendet wird in diesem Test nur die Web-Browsings Funktion des Skripts.

Folgende Benutzeraktionen werden durchgeführt:

3.1 Automatisiertes Web-Browsing

Das GitHub Tool *„Invoke-UserSimulator“* startet automatisch den Browser und „klickt“ skriptgesteuert automatisch in bestimmten, festgelegten Intervallen, zufällig auf Links vorgegebener (d.h. ebenfalls im Skript eingetragener) Websites, um von dort aus dann (wieder zufallsgesteuert) weiter zu browsen.
Um die im Wireshark Auswertungs-Protokoll zu erwartende Menge an IP Adressanfragen durch das automatisierte Webbrowsen nicht unnötig zu vergrößern (und so die Auswertung des Wireshark-Protokolls zu erschweren), wurde für den Test nur eine Website ausgesucht und auf dieser durch das Tool automatisiert „gesurft“.
Folgende Website wurde für das automatisierte Browsen ausgewählt und verwendet, da diese Website beim Start keine Verbindungen zu anderen Host Adressen (IP Adressen) herstellt:
https://www.rki.de.
Während des Testverlaufs muss zusätzlich mit dem (zufälligen) Aufruf weiterer Websites gerechnet werden, die von der Ausgangswebsite erreichbar sind.

[5] https://github.com/ubeeri/Invoke-UserSimulator

3.2 Manuelle durchgeführte Tätigkeiten am Testsystem während des 72 Stunden Tests

Zusätzlich zum automatisierten Web-Browsing werden nach einem vorab festgelegten (und für spätere Erleichterung der Auswertung in einer Excel Tabelle erfassten) Zeitplan über 72 Stunden hinweg manuell folgende Aktivitäten am System durchgeführt:

- *Notepad* Datei erstellen, speichern, verändern und kopieren.
- *Systemsteuerung* → *Ereignisanzeige „System" Events* zufällig auswählen und ansehen.
- *Paint Datei* (Zeichnung) erstellen, speichern, verändern und kopieren.
- Dateien mehrfach von und zu einem angeschlossenen *USB Stick* kopieren und ersetzen.

Hinweis:
Es wurden bewusst keine Drittthersteller-Produkte oder Teile des Microsoft Office Pakets installiert und für die Simulation benutzt, da hier von weiterem Telemetrie-Verkehr zum Software-Hersteller auszugehen ist.

4 Auswertung der Wireshark Protokolle

Das jeweils aufgezeichnete Wireshark Protokoll des Prüfszenarios wird mittels Klartextsuche („Zeichenkette") auf das Vorhandensein der Strings

- v10c *(.vortex-win.data.microsoft.com)*
- v10. *(events.data.microsoft.com)*
- v20 (.vortex-win.data.microsoft.com)
- settings-win.data.microsoft.com

durchsucht.

Laut Microsoft wird der zu erwartende Kontakt zu den Endpunkten durch DNS-Anfragen gekennzeichnet sein (die erst außerhalb des Laborsystems bzw. des Internets, aufgelöst werden), da Microsoft die IP Adressen hinter diesen Verbindungen stetig ändert.

Im Wireshark Protokoll ist somit nur das Auffinden der oben genannten Adressen (im Klartext) entscheidend.

5 Prüfergebnis

5.1 Prüfszenario 1

Im Testzeitraum von 72 Stunden konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) keine Verbindungen zu den in Kapitel 4 genannten Adressen festgestellt werden.
Eine Übermittlung von Telemetriedaten fand in diesem Szenario somit nicht statt.

5.2 Prüfszenario 2

Im Testzeitraum von nur 30 Minuten konnten mit regelmäßiger Benutzeraktivität auf dem System (inkl. Web-Browsing) bereits Verbindungen zu v10.events.data.microsoft.com und Verbindungen zu settings-win.data.microsoft.com festgestellt werden. Diese Verbindungen konnten sogar in einem zusätzlichen 30 Minuten Test ohne jegliche Benutzeraktivität festgestellt werden.
Eine Übermittlung von Telemetriedaten fand somit erwartungsgemäß statt.

5.3 Prüfszenario 3

Im Testzeitraum von 72 Stunden konnten, mit Benutzeraktivität, auf dem System (inkl. Web-Browsing) nur Verbindungen zu settings-win.data.microsoft.com festgestellt werden.
Eine Übermittlung von Telemetriedaten, insbesondere von an v10 übermittelten Diagnosedaten, hat somit nicht stattgefunden.

6 Fazit

Durch diese Tests konnten die Aussagen der Firma Microsoft nicht widerlegt werden, dass in der oben beschriebenen Konfiguration keine Telemetriedaten übermittelt werden. Hieraus kann jedoch nicht der Schluss gezogen werden, dass eine Telemetrie-Datenübermittlung grundsätzlich nicht stattfindet. Daher sind Verantwortliche stets in der Pflicht zu prüfen, ob der Einsatz von Windows 10 auch in ihrer individuellen System- und Verarbeitungssituation datenschutzrechtlich zulässig ist.

Ein besonderes Augenmerk ist auf Verbindungen zu settings-win.data.microsoft.com zu legen, da die Möglichkeit besteht, dass über diese Verbindung Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail poststelle@lfd.niedersachsen.de

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Verteiler:

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Referat 23

Bayerisches Landesamt für Datenschutzaufsicht
Bereichsleiter Cybersicherheit und Technischer Datenschutz

Die Landesbeauftragte für den Datenschutz Niedersachsen
Referat 3

Robert Krause

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582 5697
FAX +49 228 9910 9582 5697

referat-tk12@bsi.bund.de

https://www.bsi.bund.de

Betreff: Untersuchung Windows 10 Enterprise Datenverkehr

Bezug: Windows 10 Prüfung beim BayLDA am 10./11.12.2019
Geschäftszeichen: TK 12 – 240 05 00
Datum: 28.01.2020
Seite 1 von 10

Sehr geehrte Damen und Herren,

die deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder befassen sich mit der Frage, ob und unter welchen Konfigurationsmöglichkeiten das Betriebssystem Windows 10 von Verantwortlichen in Deutschland eingesetzt werden kann. Ein besonderes Augenmerk liegt dabei auf den sogenannten Telemetriedaten, die Windows 10 automatisch an Microsoft überträgt.

Zu diesem Thema fand am 10./11.12.2019 beim Bayrischen Landesamt für Datenschutzaufsicht ein Treffen von Behördenvertretern mit Microsoft zu einem technischen Fachaustausch statt, an dem auch das BSI aus IT-Sicherheits-Perspektive teilgenommen hat. Ziel war es, zu einer Aussage zu gelangen, ob Windows 10 Enterprise datenschutzkonform betrieben werden kann. In einem Versuchsaufbau sollte zudem nachgewiesen werden, dass keine unerwünschten Daten, insbesondere keine Telemetriedaten, mehr an Microsoft übertragen werden.

Als Ergebnis konnte festgestellt werden, dass im beobachteten Zeitraum keine Daten an Microsoft übertragen wurden, bei denen von einem besonderen datenschutz- oder it-technischen Risiko auszugehen ist. Auf Grund dessen, dass im Versuchsaufbau keine Nutzerinteraktion und weitere technische Rahmenbedingungen (z.B. Domänenmitgliedschaft und Updates) nachgebildet werden konnten, wurde das Interesse geäußert, auch diese Teilaspekte nochmals zu beleuchten.

Dies hat das BSI in einem eigenen Versuchsaufbau mit Blick auf IT-Sicherheitsaspekte getan, der im Folgenden erläutert sowie die Ergebnisse vorgestellt werden sollen.

ZUSTELL- UND LIEFERANSCHRIFT: Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn

Versuchsaufbau

Über einen Untersuchungszeitraum von 72 Stunden wurden folgende Systeme in virtuellen Maschinen betrieben:

- Router (Debian 10)
  - Einsatz als Router, DHCP-Server, DNS-Server
  - Verwendung von tcpdump zur Aufzeichnung des Netzwerkverkehrs
  - Verwendung zur live-Darstellung der Datenverbindungen

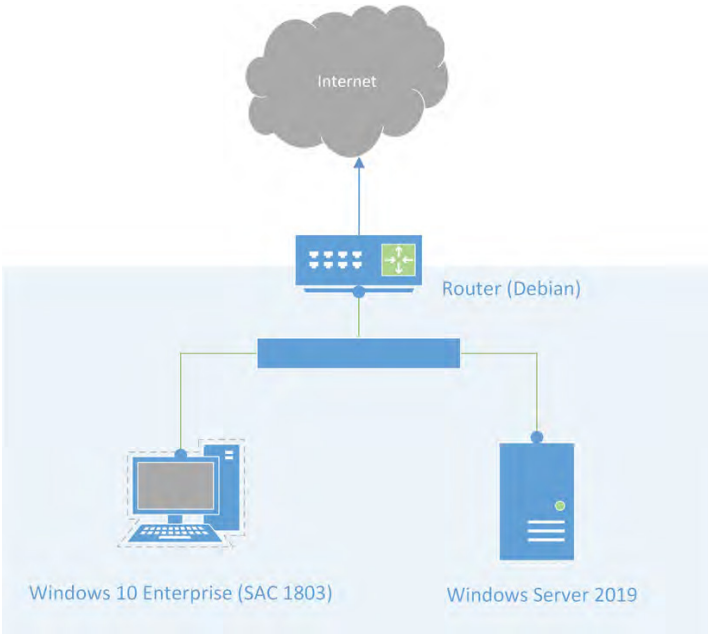
- Windows 10 Server 2019
  - Einsatz als Domaincontroller, DNS-Server, WSUS-Server
  - Bereitstellung der Gruppenrichtlinie zur Verwendung eines WSUS-Servers
  - Bereitstellung von Updates für Windows 10 SAC 1803

- Windows 10 Enterprise (SAC 1803)
  - Einsatz als Workstation
  - Anwendung der Windows Restricted Traffic Limited Functionality Baseline[1] für Windows 10 SAC 1803
  - Domänen-Mitglied
  - Bezug von Updates über WSUS-Server der Domäne
  - Verwendung von Fiddler und procmon zur lokalen Systemüberwachung
  - Deaktivierung des Zertifikat-Pinnings durch Setzen des Schlüssels „SkipMicrosoftRootCertCheck“ in HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Diagnostics/DiagTrack/TestHooks auf DWORD 0x1
  - Simulation von Nutzer- und Systemverhalten
    - Regelmäßige Prüfung auf Updates und deren Installation
    - Regelmäßige Neustarts
    - Simulation von Systemauslastung und Abstürzen (via Sysinternal Suite)
    - Starten und Verwenden von Programmen (ohne Internetfunktionen), z.B. Wordpad, Notepad, Powershell, Systemkommandos
    - De- und Installation weiterer Programme, Rekonfiguration der Einstellungen per GUI

1 https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

Bundesamt
für Sicherheit in der
Informationstechnik

Das Netzwerkdiagramm stellt sich wie folgt dar:



Ergebnis

Im gesamten Untersuchungszeitraum haben 2741 Pakete (1.919.128 Bytes) das Netzwerk über den Router hinaus zum Internet hin verlassen. Im Detail sind dabei folgende Endpunkte adressiert worden:

119 packets	26991 bytes	Microsoft Store Images (store-images.s-microsoft.com)	(23.210.254.117)
1931 packets	1594376 bytes	[u'www.fiddler2.com', u'fiddler2.com']	(50.56.19.116)
11 packets	2561 bytes	a2-22-119-98.deploy.static.akamaitechnologies.com	(2.22.119.98)
12 packets	2159 bytes	Microsoft.com Website (www.microsoft.com)	(23.210.253.93)
76 packets	11159 bytes	a2-22-119-33.deploy.static.akamaitechnologies.com	(2.22.119.33)
59 packets	13467 bytes	a2-22-89-31.deploy.static.akamaitechnologies.com	(2.22.89.31)
344 packets	123752 bytes	Windows Apps dynamic configuration update (settings-win.data.microsoft.com)	(40.74.35.71)
123 packets	126499 bytes	UNKNOWN	(52.155.217.156)
15 packets	3195 bytes	a2-22-94-250.deploy.static.akamaitechnologies.com	(2.22.94.250)
51 packets	14969 bytes	a2-19-241-220.deploy.static.akamaitechnologies.com	(2.19.241.220)

Diese sollen nun gesondert betrachtet werden.

50.56.19.116 – fiddler2.com – 1.6 MB / 1931 Pakete

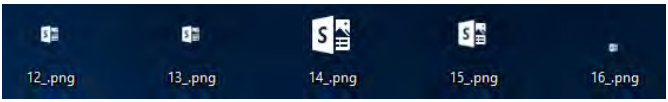
Diese IP wurde jeweils beim Starten der Anwendung „Fiddler2“ abgerufen und dient der Überprüfung und dem Bezug von Aktualisierungen. Es handelt sich um eine Verbindung, die nicht Microsoft Windows zuzurechnen ist und kann daher bei dieser Untersuchung unbeachtet bleiben.

23.210.254.117 – store-images.s-microsoft.com – 27 KB / 119 Pakete

Über den gesamten Zeitraum sind Verbindungen zum Bildarchiv des Microsoft Stores zu verzeichnen.

15	200	HTTP	store-images.microsoft.com	/image/apps.15158.9007199267163071.05e06c13-c5a6-4b55-aa49-95ac316ff92b.43c68c78-a422-4b09-acc3-77e6028d568f
16	200	HTTP	store-images.microsoft.com	/image/apps.14793.9007199267163071.55f83110-ba62-4b6a-bc0a-8f12f27a5bb9.361cbfef-c19c-41d3-8a02-b1e3c8b2d188
17	200	HTTP	store-images.microsoft.com	/image/apps.63578.9007199267163071.f2756185-4638-47e0-9958-1ed9aa60f2a0.7480e404-ca1b-478b-846a-0b8514815b60
18	200	HTTP	store-images.s-microsoft.com	/image/apps.11611.9007199267163071.051d6f39-e04c-4c03-be99-103ab2771658.78beb32a-1635-487b-8355-2003309e37cf
19	200	HTTP	store-images.s-microsoft.com	/image/apps.47093.9007199267163071.afa2c461-b588-4b32-97c1-b7daddc7d914.9e65fb00-e27b-4e87-b6aa-c6626c8503b1

Im Detail handelt es sich dabei um das Herunterladen von Bildern, u.a. von der Anwendung „Office Sway“, bei der es sich um eine Präsentations-Webanwendung handelt. Grund dafür ist vermutlich, die Anwendung als Schnellzugriff im dynamischen Startmenü von Windows anzubieten zu können.



Bundesamt
für Sicherheit in der
Informationstechnik

Neben den Bilddaten, sind im Rahmen der Datenverbindung folgende Informationen übertragen worden.

Diese Verbindung ist unerwartet, da davon ausgegangen wurde, dass sämtliche Verbindungen zum Microsoft Store durch Anwendung der Windows Restricted Traffic Limited Functionality Baseline unterbunden bzw. deaktiviert sind.

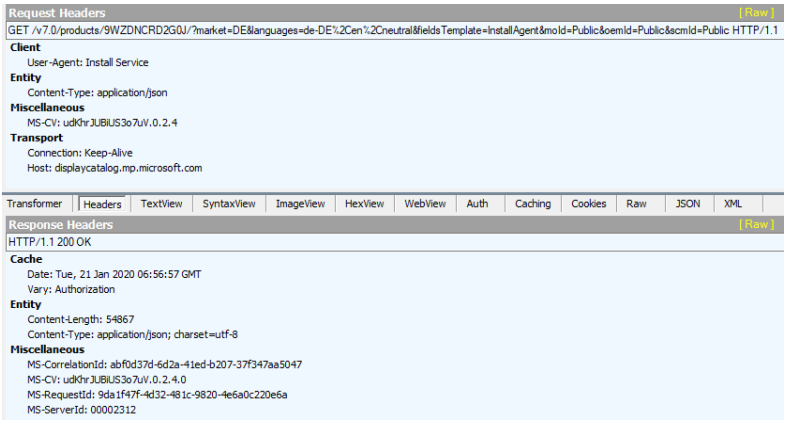
Dennoch geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

52.155.217.156 – displaycatalog.mp.microsoft.com – 126 KB / 123 Pakete

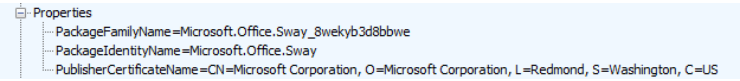
Im Zusammenhang mit der Überprüfung auf Updates konnten regelmäßig Verbindungen zur Domain „displaycatalog.mp.microsoft.com“ festgestellt werden, die die Grundlage zum vorher genannten Abruf der Bilddaten von „store-images.s-microsoft.com“ darzustellen scheint.

Bundesamt
für Sicherheit in der
Informationstechnik

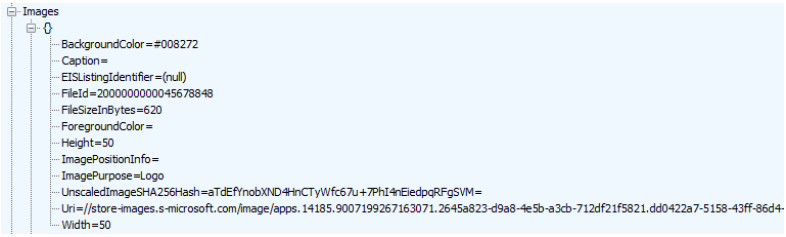
Die Kopfdaten der Verbindung stellen sich wie folgt dar:



Als Antwort erhielt der Client Informationen zu von Microsoft angebotenen Produkten; hier zu Office Sway in JSON-kodierter Form.



Dabei sind u.a. auch die Links zu den im Bildarchiv des Microsoft-Stores abgerufenen Icons zu finden.



Auch wenn diese Verbindung unerwünscht ist und i.R. der Windows Restricted Traffic Limited Functionality Baseline nicht auftreten sollte, kann auf Grund der wenigen Daten, die der Client selbst sendet und dem Inhalt der empfangenen Daten keine Gefährdung erkannt werden.

23.210.253.93 – crl.microsoft.com – 2 KB / 12 Pakete

Hierbei handelt es sich um eine Verbindung zur Certificate Revocation List (CRL) bei Microsoft, um zu prüfen, ob Zertifikate gesperrt oder widerrufen wurden. Diese Verbindung konnte im Untersuchungszeitraum nur einmal beobachtet werden, nämlich nach dem erstmaligen Start der Anwendung „procmon". Dieses Programm ist mit einem Zertifikat signiert, um die Echtzeit nachzuweisen. In diesem Zusammenhang hat Windows offensichtlich die CRL kontaktiert.

Der nachfolgende Screenshot zeigt die Eigenschaften der Verbindung.

```
GET /pkiops/crl/MicCodSigPCA2011_2011-07-08.crl HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/10.0
Host: www.microsoft.com

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 813
Content-MD5: w9MsPQooRx3ylPz3q1ix5w==
Last-Modified: Mon, 13 Jan 2020 06:00:56 GMT
ETag: 0x8D797EDF4BC8643
x-ms-request-id: 46820ea4-b01e-0001-12db-c9468d000000
x-ms-version: 2009-09-19
x-ms-lease-status: unlocked
x-ms-blob-type: BlockBlob
Date: Wed, 15 Jan 2020 07:03:28 GMT
TLS_version: UNKNOWN
X-RTag: RT
X-Cache: MISS from dsl-ga.tn-ga
X-Cache-Lookup: HIT from dsl-ga.tn-ga:800
Connection: keep-alive
```

Auch hier geben die übertragenen Daten keinen Anlass, darin ein Risiko bzw. ein Offenlegen vertrauenswürdiger Informationen zu sehen.

2.22.119.98 / 2.22.119.33 / 2.22.89.31 / 2.22.94.250 / 2.19.241.220
***.deploy.static.akameitechnologies.com – 45 KB / 212 Pakete**

Bei diesen IP-Adressen und Domains handelt es sich um ein Content Delivery Network (CDN) von Akamei, das der Auslieferung und Beschleunigung von Online-Anwendungen dient. Diese Endpunkte stellen Aliase dar, den anderen, hier bereits analysierten Endpunkten entsprechen.

2.22.119.98 → crl.microsoft.com
2.22.119.33 → crl.microsoft.com

2.22.94.250 → store-images.microsoft.com
2.22.89.31 → store-images.microsoft.com
2.19.241.220 → store-images.microsoft.com

40.74.35.71 – settings-win.data.microsoft.com – 124 KB / 344 Pakete

Diese Verbindung wird vom System regelmäßig – vorrangig vor dem Überprüfen auf Windows Updates – hergestellt.

Auffällig bei dieser Verbindung war, dass sie zunächst nur auf dem Router und nicht im lokalen Proxy beobachtet werden konnte. Der per GUI / Fiddler in Windows konfigurierte Proxy-Server wurde nicht verwendet. Vielmehr war es notwendig, eine weitere Konfiguration über das Kommando „netsh winhttp set proxy" vorzunehmen.

Anschließend konnte der Aufbau der Verbindung zwar in Fiddler beobachtet werden, die Verbindung selbst hat jedoch keinerlei Nutzdaten mehr übertragen, was auf die Verwendung von Zertifikats-Pinnung durch Microsoft hindeutet.

Weitere Versuche, an den unverschlüsselten Datenverkehr zu gelangen, wurden nicht unternommen. Zu den Inhalten dieser Verbindung kann daher keine Aussage getroffen werden.

Nach Angaben[2] von Microsoft würden Apps diesen Endpunkte verwenden, um ihre Konfiguration dynamisch zu aktualisieren. So seien u.a. die Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus" und das „Windows-Insider-Programm" betroffen.

Auch im BSI-Projekt „SiSyPHuS"[3] ist diese Domain mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt. Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne

2 https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
3 https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

dass der Nutzer dem Zustimmen muss oder das kontrollieren kann. Vor diesem Hintergrund sind Verbindungen zu diesem Endpunkt zumindest als bedenklich einzustufen.

Auf Nachfrage ist im Gespräch mit Microsoft am 10./11.12.2019 in Ansbach mündlich bestätigt worden, dass die in dieser Verbindungen übertragenen Daten nach Anwendung der Windows Restricted Traffic Limited Functionality Baseline (und damit des Telemetrielevels „Security") von der Windows-Telemetriekomponente nicht weiter verwendet werden würden und das Abrufen allein technische Ursachen in der Implementierung habe.

Was diese Datenverbindung tatsächlich überträgt und ob damit sicherheits- oder datenschutzrelevante Konfigurationen am System vorgenommen werden, kann, mangels Einblick in den Datenverkehr, nicht bewertet werden.

Bewertung

Im Rahmen dieser Untersuchung haben sich keine Hinweise ergeben, dass Windows 10 Enterprise mit der Konfiguration „Windows Restricted Traffic Limited Functionality Baseline" Daten an Microsoft übertragen hat, die aus h.S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden.

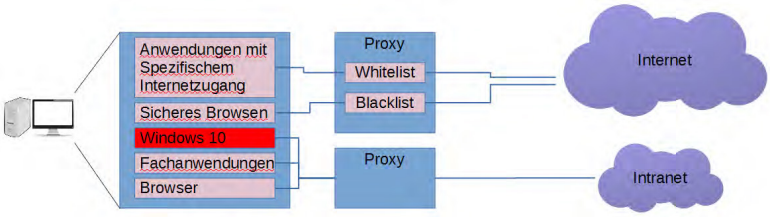
Dabei ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com" nicht im Klartext analysiert werden konnten und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt.

Darüber hinaus stellt diese Untersuchung nur eine Momentaufnahme für eine explizite Version von Windows 10 Enterprise in diesem Patchstand und einer speziellen Konfiguration dar. Durch weitere Updates und Änderungen am System durch Microsoft oder Konfigurationen des Nutzer kann sich dieses Verhalten verändern. Eine regelmäßige Aktualisierung und Prüfung der Untersuchungsergebnisse ist daher erforderlich.

Trotz der gewonnenen Erkenntnisse wird die Empfehlung des BSI, Windows 10 im Rahmen einer Netztrennung zu betreiben aufrecht erhalten. Grund dafür ist einerseits die Möglichkeit, dass sich das festgestellte Systemverhalten jederzeit durch Updates oder Konfigurationsänderungen des Herstellers ändern kann. Insbesondere die Nichtbewertbarkeit der bei der dynamischen Konfiguration der Telemetrie beteiligten Verbindung zu „settings-win.data.microsoft.com" zeigt, dass keine belastbare, abschließende Aussage möglich ist und weitere Datenkommunikation auftreten kann. Andererseits wird mit der Netztrennung eines Systems dem Grundsatz „Defence in depth" Rechnung getragen. So können nicht nur möglicherweise auftretende, unerwünschte Datenübertragungen von Anwendungen auf dem System verhindert, sondern auch wirkungsvoll die Exfiltration von Daten z.B. durch Malware vorgebeugt werden.

Bundesamt
für Sicherheit in der
Informationstechnik

Seite 10 von 10



Dennoch bewirkt die Anwendung der Windows Restricted Traffic Limited Functionality Baseline für Windows 10 Enterprise einen deutlich verminderten Umfang an Daten, die in das Internet übertragen werden. Eine ähnliche Konfigurationsmöglichkeit auch für Windows 10 Pro/Home wäre wünschenswert.

Dabei ist jedoch – entsprechend der Benennung der Richtlinie – ein verminderter Funktionsumfang zu verzeichnen. So konnten beispielsweise im Rahmen der Untersuchung keine Anwendungen mehr gestartet werden, die Bezüge zum Windows Store haben. Die Auswirkungen auf die Praxistauglichkeit dieser Richtlinie werden auf Grund der Testergebnisse jedoch als eher gering bewertet.

Im Auftrag

Dr. Wippig

2.2
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 22.09.2020

Anwendung der DSGVO auf Datenverarbeitungen von Parlamenten

Anlässlich des Urteils des EuGH vom 9. Juli 2020 (C-272/19) wird der Beschluss der Datenschutzkonferenz vom 5. September 2018 „Anwendung der DSGVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien“ bis zur Neuformulierung eines Beschlusses ausgesetzt.

2.3
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 10.09.2020

Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie

I. AUSGANGSLAGE

Da eine SARS-CoV-2-Infektion teilweise mit einer spezifisch erhöhten Körpertemperatur der infizierten Person einhergeht, werden zunehmend elektronische Geräte zur Temperaturerfassung als Mittel der Zutrittssteuerung zu bis dahin öffentlich zugänglichen Räumen oder zu Arbeitsstätten eingesetzt.

Eine kontaktlose Temperaturmessung erfolgt in der Regel per Infrarotmessung und wird entweder mithilfe eines Fieberthermometers oder einer Thermalkamera / Infrarot-Wärmebildkamera[1] vorgenommen. In den nunmehr angedachten Szenarien für den Zugang zu Flughäfen, Geschäften, Behörden, Arbeitsstätten etc. wird insbesondere die Nutzung von Wärmebildkameras in Betracht gezogen, da mittels klassischer Fieberthermometer keine Temperaturmessung bei größeren Gruppen erfolgen kann. Sie kann höchstens für die Messung von Einzelpersonen nacheinander, wie z. B. in Vereinzelungsschleusen, zum Einsatz kommen, wobei bei einer einzelnen Fiebermessung mittels Thermometer ohne Protokollierung abhängig vom Einsatzszenario die Anwendbarkeit der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) in Frage stehen kann. **Einzelhandelsunternehmen und Behörden setzen**

1 Sofern im Folgenden allein der Einsatz von Wärmebildkameras oder der elektronischen Temperaturerfassung thematisiert wird, beziehen sich die Ausführungen grundsätzlich stets auf beide Verarbeitungsarten.

bereits vergleichbare Wärmemessungen ein, um den Zutritt zu ihren Geschäftsräumen zu regulieren.

ANWENDUNGSBEREICH DES BESCHLUSSES

Der Beschluss betrifft den Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung zur Steuerung oder aus Anlass des Zugangs zu Flughäfen, Geschäften, Behörden und Arbeitsstätten im Rahmen der Corona-Pandemie. Einrichtungen im Bereich der Gesundheitsversorgung einschließlich der Pflege können besonderen Maßnahmen unterliegen.

II. ZUSAMMENFASSUNG

Für die elektronische Messung der Körpertemperatur zur allgemeinen Regulierung des Zutritts zu Flughäfen, Geschäften, Behörden und Arbeitsstätten kann zwar Art. 6 Abs. 1 UAbs. 1 Buchst. e, Art. 9 Abs. 2 DSGVO i. V. m. § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutzgesetzen (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) bzw. Art. 6 Abs. 1 UAbs. 1 Buchst. f, Art. 9 Abs. 2 DSGVO (Verfolgung eines berechtigten Interesses) als Rechtsgrundlage in Betracht kommen. Auch ist die Messung als betriebliche Maßnahme des Arbeitsschutzes bzw. zur Beurteilung der Arbeitsfähigkeit gestützt auf Art. 88 DSGVO i. V. m. § 26 Abs. 3 BDSG (bzw. das Personaldatenschutzrecht des jeweiligen Landes) bzw. § 22 Abs. 1 Nr. 1 Buchst. b BDSG i. V. m. Art. 9 Abs. 2 DSGVO grundsätzlich denkbar. Jedoch fehlt es i. d. R. an der Eignung und der Erforderlichkeit der Messung. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden und viele Infizierte weisen keine Symptome und damit auch keine erhöhte Temperatur auf. Zudem sind mildere Maßnahmen wie z. B. die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der Beschäftigten durch den Arbeitgeber denkbar.

III. DATENSCHUTZRECHTLICHE BEWERTUNG

Die elektronische Messung der Körpertemperatur fällt – jedenfalls typischerweise – in den **Anwendungsbereich** der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO).

Die Messung der Körpertemperatur eines Menschen stellt eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 und Nr. 2 DSGVO dar.

Lässt ein Verantwortlicher Körpertemperaturmessungen an Personen vornehmen, sind hierdurch regelmäßig **personenbezogene Daten** betroffen.

Zwar erfassen die Temperaturmessungen selbst noch keine eindeutig identifizierenden Angaben wie Namen und Anschriften der Personen, die eine entsprechende Messeinrichtung passieren. Typischerweise kann jedoch die betroffene Person dabei anderweitig identifiziert werden, etwa durch Personal, das die Messungen und eventuell Aufzeichnungen vornimmt, durch den Einsatz von Videokameras oder durch Arbeitszeiterfassungsgeräte. Anderes könnte allenfalls gelten, wenn eine automatisierte Temperaturmessung stattfindet, die vollkommen ohne Protokollierung und ohne anderweitige Zuordnung der Werte zu bestimmten oder bestimmbaren Personen erfolgt. Im Zusammenhang mit der Corona-Pandemie würde eine solche Messung allerdings ihren präventiven Zweck verfehlen.

In aller Regel sind die mithilfe einer automatisierten Temperaturmessung erzeugten Daten also personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO. Erst recht unterstützt die Speicherung von Infrarotkamera-Aufnahmen eine nachträgliche persönliche Identifikation betroffener Personen. Wird eine Wärmebilderfassung gar mit einer herkömmlichen Videoüberwachung verknüpft, ist generell von einem Personenbezug der Bildaufnahmen auszugehen (vgl. BVerwG, Urteil vom 27.03.2019, Az. 6 C 2/18, Absatz 43 der Entscheidungsbegründung).

Die Anwendung der Datenschutz-Grundverordnung setzt nach Art. 2 Abs. 1 DSGVO weiterhin voraus, dass entweder eine automatisierte **Verarbeitung** oder eine nichtautomatisierte Verarbeitung personenbezogener Daten erfolgt, die in einem Dateisystem gespeichert werden oder werden sollen.

> Beispiel: Die Erfassung der Körpertemperatur mithilfe eines Wärmebildkamerasystems ist eine automatisierte Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO – unabhängig davon, ob die Aufnahmen gespeichert werden oder ob ein Live-Monitoring erfolgt (vgl. BVerwG, Urteil vom 27.03.2019, a. a. O., Absatz 43 der Entscheidungsbegründung).

Ausgehend von den beschriebenen Einsatzbedingungen der elektronischen Temperaturerfassung setzen die nachfolgenden Ausführungen die Anwendbarkeit der Datenschutz-Grundverordnung voraus. Sie beziehen sich allerdings nicht auf solche Temperaturmessungen, für die der Anwendungsbereich der Datenschutz-Grundverordnung ausnahmsweise nicht eröffnet ist.

Da die elektronische Temperaturmessung darauf gerichtet ist, Personen zu identifizieren, die mit SARS-CoV-2 infiziert sind, handelt es sich um eine Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO. Soweit eine solche Verarbeitung von personenbezogenen Gesundheitsdaten erfolgt, ist sie nach Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Dieses **grundsätzliche Verarbeitungsverbot** gilt nur dann nicht, wenn die Verarbeitung einen Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO erfüllt.

Im Folgenden werden daher die je nach Anwendungsfall in Betracht kommenden Rechtsgrundlagen näher untersucht, beginnend mit den allgemeinen Verarbeitungsbefugnissen.

Dabei ist neben dem grundsätzlichen Verarbeitungsverbot und den Ausnahmetatbeständen des Art. 9 DSGVO zu beachten, dass eine Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 Buchstabe a, Art. 6 Abs. 1 UAbs. 1 DSGVO nur dann rechtmäßig ist, wenn sie mindestens auf eine **Rechtsgrundlage** im Sinne des Art. 6 Abs. 1 DSGVO gestützt werden kann. Bei der elektronischen Temperaturmessung ist dies regelmäßig **nicht** gegeben. Folgende Erwägungen sind diesbezüglich zu beachten:

– Eine **Einwilligung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe a DSGVO kann nur wirksam erteilt werden, wenn die Voraussetzungen der Art. 4 Nr. 11, Art. 7 DSGVO erfüllt sind (zu Einzelheiten vgl. Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DSGVO; Europäischer Datenschutzausschuss, WP 259 rev. 01: Leitlinien in Bezug auf die Einwilligung gemäß Verordnung EU 2016/679). Zudem ist zu beachten, dass die Wärmemessung gerade der Erfassung einer etwaigen Erkrankung dient; deshalb hat die betroffene Person ihre Einwilligung ausdrücklich zu erklären (vgl. Art. 9 Abs. 2 Buchstabe a DSGVO).
  Im Zusammenhang mit der Zielsetzung der Zutrittsregulierung mithilfe von Wärmebildmessungen wird die Einwilligung als Verarbeitungsgrundlage schon in praktischer Hinsicht oft ausscheiden, weil es an der **Freiwilligkeit** der Zustimmungserklärung fehlt. Zudem wird die Wirksamkeit der Einwilligung häufig auch daran scheitern, dass eine transparente **Information** der betroffenen Person vor Durchführung des Messvorganges in der Praxis zweifelhaft scheint.

  Beispiel: Zahlreiche Beschäftigungsverhältnisse sind stark von einem Ungleichgewicht zwischen den Beschäftigten und ihrem Arbeitgeber bzw. Dienstherrn geprägt (Erwägungsgrund 43 DSGVO). Vor diesem Hintergrund werden die Beschäftigten kaum eine vom Vorgesetzten etablierte Zutrittskontrolle verweigern können, wenn sie zu ihrem Arbeitsplatz gelangen wollen. Anderes kann ausnahmsweise gelten, wenn Arbeitgeber

bzw. Dienstherren etwa mithilfe von Betriebs- bzw. Dienstvereinbarungen die Rahmenbedingungen für die Freiwilligkeit einer Einwilligungserklärung von Beschäftigten festlegen.

Beispiel: Die Zutrittsregelung betreffend Behörden- oder Gerichtsgebäude kann typischerweise nicht auf die Einwilligung gestützt werden, sofern die betroffenen Personen eine gesetzlich vorgesehene, staatliche Leistung in Anspruch nehmen wollen oder gar auf behördliche oder gerichtliche Ladung hin den Zutritt zum jeweiligen Gebäude begehren. Denn insoweit ist die Freiwilligkeit einer Zustimmung stets zweifelhaft und kann durch den Verantwortlichen regelmäßig nicht belegt werden (vgl. Art. 7 Abs. 1, Erwägungsgrund 43 DSGVO).

Beispiel: In Bezug auf den Zutritt zum Geschäftslokal eines Unternehmens wird die Einholung einer hier nach Art. 9 Abs. 2 Buchstabe a DSGVO rechtlich gebotenen ausdrücklichen Einwilligung der Kunden häufig bereits aus pragmatischen Erwägungen nicht in Frage kommen. Zudem hängt die Freiwilligkeit auch dann von den Umständen des Einzelfalls ab, wobei die gesetzliche Wertung des Art. 7 Abs. 4 DSGVO zu beachten ist.[2] Soweit der Zutritt zum Geschäftslokal an die Einwilligung zur Temperaturmessung geknüpft wird, kann also nicht ohne weiteres von einer Freiwilligkeit ausgegangen werden.

– Auch Art. 6 Abs. 1 UAbs. 1 Buchstabe b DSGVO scheidet als Rechtsgrundlage in aller Regel aus. Bei Zugangskontrollen erfolgt die Temperaturmessung nicht zur Erfüllung eines bestehenden Vertragsverhältnisses zwischen den Parteien.
– Als Verarbeitungsgrundlage kommt der Vertrag am ehesten **bei Beschäftigungsverhältnissen im nichtöffentlichen Sektor und bei Tarifbeschäftigten des öffentlichen Sektors** in Betracht. Insoweit sieht Art. 9 Abs. 2 Buchstabe b DSGVO unter den dort festgelegten Voraussetzungen u. a. eine Ausnahme vom Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO vor, soweit der Verantwortliche oder die betroffene Person einer aus dem Arbeitsrecht folgenden Pflicht nachkommen muss. In Bezug auf die elektronische Temperaturmessung bei Beschäftigten kommt allenfalls in Betracht, dass mit ihr der Arbeitgeber bzw. Dienstherr seine aus dem Arbeitsschutzrecht folgenden Pflichten erfüllen will.

2 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Rn. 14

Eine solche vertragliche Befugnis zur Temperaturmessung kann allerdings nicht weiter reichen als eine rechtliche Verpflichtung des Verantwortlichen im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO.

– Teilweise berufen sich Unternehmen bei der Temperaturmessung darauf, sie sei erforderlich, um eine **rechtliche Verpflichtung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO zu erfüllen. Diese Vorschrift stellt selbst keine rechtliche Verarbeitungsgrundlage dar, sondern setzt gemäß Art. 6 Abs. 2, Abs. 3 UAbs. 1 DSGVO eine Rechtsgrundlage im bereichsspezifischen EU-Recht oder im Recht eines Mitgliedstaates voraus. Die in dieser Vorschrift normierte Verpflichtung muss sich unmittelbar auf die Verarbeitung personenbezogener Daten beziehen. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus (vgl. z. B. LSG Hessen, Beschluss vom 29.01.2020, Az. L 4 SO 154/19 B, Absatz 13 der Entscheidungsgründe).
  Eine solche rechtliche Verpflichtung der Unternehmen zur Temperaturmessung ist im deutschen Recht nicht ausdrücklich vorgesehen. In Beschäftigungsverhältnissen verpflichtet § 3 Abs. 1 Arbeitsschutzgesetz den Arbeitgeber zwar allgemein dazu, die erforderlichen Maßnahmen des Arbeitsschutzes „*unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen*“. Ferner ist der Arbeitgeber nach § 618 Bürgerliches Gesetzbuch grundsätzlich verpflichtet, Maßnahmen zum Schutz von Leben und Gesundheit seiner Beschäftigten zu ergreifen. Aus diesen allgemeinen gesetzlichen Vorgaben zum betrieblichen Gesundheitsschutz lässt sich jedoch gerade nicht eine konkrete rechtliche Pflicht im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO ableiten, den Zugang zum Betriebsgelände mithilfe einer elektronischen Temperaturmessung zu regulieren.
  Auch unter Berücksichtigung des am 16. April 2020 durch das Bundesministerium für Arbeit und Soziales veröffentlichten „Arbeitsschutzstandard SARS-CoV-2“ oder der sonstigen bereichs- und branchenspezifischen Arbeitsschutzstandards ergibt sich nichts anderes. Ungeachtet dessen, dass darin Temperaturmessungen als betriebliche Maßnahme in Betracht gezogen werden sollen (II. Nr. 13 des Arbeitsschutzstandards SARS-CoV-2: „*insbesondere Fieber, Husten und Atemnot … Anzeichen für eine Infektion mit dem Coronavirus sein (können). Hierzu ist im Betrieb eine möglichst kontaktlose Fiebermessung vorzusehen.*“), begründen sie keine rechtliche Verpflichtung des Arbeitgebers oder Dienstherrn im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, im Wege der Fiebermessung personenbezogene Daten zu verarbeiten. Denn die Arbeitsschutzstandards SARS-CoV-2 sind kein Rechtssatz, aus denen eine rechtliche

Verpflichtung folgt, sondern eine Art Leitlinie der öffentlichen Verwaltung zum Arbeitsschutz.

Damit existiert gegenwärtig keine spezifische rechtliche Verpflichtung für Verantwortliche im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, elektronische Fiebermessungen durchzuführen.

– Art. 6 Abs. 1 UAbs. 1 Buchstabe d DSGVO gestattet die Verarbeitung personenbezogener Daten, wenn sie erforderlich ist, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen. Bei der im Raum stehenden Verarbeitung von personenbezogenen Gesundheitsdaten durch elektronische Temperaturmessung muss allerdings gem. Art. 9 Abs. 2 Buchstabe c DSGVO die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande sein, ihre Einwilligung in die Verarbeitung zu geben, so dass diese Rechtsgrundlage **nicht** herangezogen werden kann.
– Hingegen kommt in einzelnen Fällen in Betracht, dass die Temperaturmessung für die Wahrnehmung einer **im öffentlichen Interesse liegenden Aufgabe** erforderlich ist, die dem Verantwortlichen übertragen wurde. Dazu stellt Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO selbst keine Verarbeitungsbefugnis dar, sondern setzt nach Art. 6 Abs. 2 und 3 UAbs. 1 DSGVO eine Rechtsgrundlage voraus. Eine solche Verarbeitungsgrundlage kann grundsätzlich auch in einer Generalklausel bestehen; insbesondere muss sie von EU-Rechts wegen nicht, wie bei der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, konkret den Verarbeitungszweck enthalten. Es genügt nach Art. 6 Abs. 3 UAbs. 2 DSGVO, wenn der Zweck der Verarbeitung erforderlich ist, um eine Aufgabe zu erfüllen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies setzt immerhin voraus, dass eine solche Aufgabe im Recht des Mitgliedstaats so klar und konkret beschrieben wird, dass aus ihr rechtssicher ein zulässiger Verarbeitungszweck abgeleitet werden kann. Insbesondere darf die gesetzliche Zuständigkeits- und Aufgabenordnung nicht durch zu unbestimmte Verarbeitungsregeln unterlaufen werden.
  Daraus folgt, dass die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 Buchstabe i DSGVO, § 22 Abs. 1 Nr. 1 Buchstabe c Bundesdatenschutzgesetz (BDSG) keine allgemeine Befugnis von Behörden für die Verarbeitung von Gesundheitsdaten begründet. Diese Vorschriften beziehen sich ihrem Wortlaut und ihrer Entstehungsgeschichte nach auf das öffentliche Gesundheitswesen und auf die Gesundheitsverwaltung.
  Dient die Temperaturmessung allerdings der allgemeinen **Zutrittsregulierung zu Gebäuden der öffentlichen Verwaltung**, kommt mangels bereichsspezifischer Vorschriften der Rückgriff auf die datenschutzrecht-

lichen Generalklauseln in § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutzgesetzen in Betracht. Anknüpfungspunkt wäre insoweit die Aufgabe einer jeder öffentlichen Stelle, einen ordnungsgemäßen – das heißt auch für Besucherinnen und Besucher sowie Beschäftigte möglichst gefahrlosen – Dienstbetrieb zu gewährleisten. Zusätzlich muss eine Verarbeitungsbefugnis im Hinblick auf die nach Art. 9 Abs. 2 DS-GVO besonders geschützten Gesundheitsdaten vorliegen (etwa, soweit anwendbar, § 22 Abs. 1 Nr. 1 Buchstabe d BDSG). Dabei ist regelmäßig der Grundsatz der Erforderlichkeit zu berücksichtigen, anhand dessen zu prüfen ist, ob das Fiebermessen tatsächlich erforderlich und zielführend zur Erreichung des Zwecks ist. Für die Prüfung der Erforderlichkeit sind Konzepte zu erstellen, die die beabsichtigten Maßnahmen und die damit verfolgten Zwecke schlüssig und nachvollziehbar darlegen. Zusätzlich haben die Behörden dabei die besonderen Regeln zum Schutz sensibler Daten zu beachten. An der Eignung und Erforderlichkeit einer elektronischen Fiebermessung bestehen allerdings erhebliche Zweifel; diese werden weiter unten im Zusammenhang mit den Ausführungen zu Art. 6 Abs. 1 UAbs.1 Buchstabe f DSGVO näher erörtert.

Die Steuerung des Zutritts zu öffentlichen Verkaufsflächen von Unternehmen lässt sich hingegen regelmäßig **nicht** auf Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO in Verbindung mit der jeweiligen mitgliedstaatlichen Befugnisnorm stützen. **Unternehmen und andere nichtöffentliche Verantwortliche** können sich auf diese Vorschrift nur berufen, wenn ihnen eine Verarbeitungsbefugnis im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt „übertragen" ist. Sie müssen anstelle einer Behörde tätig werden, was einen wie auch immer gearteten staatlichen Übertragungsakt voraussetzt. Mit anderen Worten können sich Privatpersonen nicht selbst zum Sachwalter eines öffentlichen Interesses erklären. Deshalb scheidet die Wahrnehmung einer öffentlichen Aufgabe im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO für nichtöffentliche Verantwortliche gegenwärtig als Verarbeitungsgrund aus (vgl. BVerwG, Urteil vom 27.03.2019, a. a. O., Absatz 46 der Entscheidungsbegründung).

– Für Unternehmen und andere nichtöffentliche Stellen steht allerdings Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO zur Verfügung, der – verkürzt ausgedrückt – eine **Verarbeitung auf Grundlage einer Interessenabwägung** dann erlaubt, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und nicht die Interessen der betroffenen Person überwiegen. Verantwortliche des öffentlichen Sektors können sich im Rahmen ihrer Aufgabenerfüllung nicht auf diese Verarbeitungsgrundlage stützen, vgl. Art. 6 Abs. 1 UAbs. 2 DSGVO.

Im Zusammenhang mit der elektronischen Fiebermessung ist wiederum zu beachten, dass sie als Verarbeitung personenbezogener Gesundheitsdaten nur zulässig sein kann, wenn eine Ausnahme vom grundsätzlichen Verarbeitungsverbot nach Art. 9 Abs. 2 DSGVO besteht. Eine solche Ausnahme ist jedoch allenfalls in seltenen Ausnahmefällen denkbar.
Die Verarbeitungsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO setzt nach gefestigter Rechtsprechung drei Prüfschritte voraus (vgl. u. a. EuGH, Urteil vom 04.05.2017, Az. C-13/16, Absatz 28 der Entscheidungsgründe):
Erstens muss die Verarbeitung ein berechtigtes Interesse verfolgen, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht das Verarbeitungsinteresse des Verantwortlichen überwiegen.
Ein **berechtigtes Verarbeitungsinteresse** ist vorliegend zu bejahen, soweit die mit der elektronischen Fiebermessung verbundene Erhebung von Daten zur Abwehr von Gefährdungen für die Belegschaft bzw. der übrigen Kundschaft und damit auch der Aufrechterhaltung des Geschäftsbetriebs dienen soll.
Die **Erforderlichkeit** der Maßnahme hingegen ist regelmäßig nicht zu bejahen. Soweit die Veröffentlichung der Datenschutzkonferenz „Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie“ insoweit für die Ermittlung der Erforderlichkeit verallgemeinerungsfähig darauf hinweist, dass – unter Beachtung des Gebots der Verhältnismäßigkeit – die „*Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern legitim sein könne, insbesondere um festzustellen, ob diese selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen oder sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben*“, beschränkt sich dies auf die zulässige Datenverarbeitung im **unmittelbaren Kontext** der mit dem Pandemiegeschehen verbundenen Gesundheitsgefahren. Vor diesem Hintergrund sind Befragungen und auch weitergehende Maßnahmen nicht generell ausgeschlossen, allerdings ist das Tatbestandsmerkmal der Erforderlichkeit im spezifischen Verarbeitungszusammenhang zu beachten.
Bei der Erforderlichkeitsprüfung ist zu beachten, dass eine erhöhte Körpertemperatur nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-

Infektion angesehen werden kann. Sie kann auch durch zahlreiche andere Ursachen, wie etwa Erkältungen, Stoffwechsel- und Gefäßerkrankungen, Rheuma, entzündliche Prozesse bedingt sein. Zudem weisen nach Angaben des Robert-Koch-Instituts (RKI) nur etwa 41 Prozent der Infizierten einen Krankheitsverlauf mit Fieber auf; in der bis zu 14 Tage umfassenden Inkubationszeit weisen die infizierten Personen noch keine Symptome auf oder bleiben über den gesamten Infektionsverlauf vollständig symptomfrei, sind aber aufgrund der Viruslast potenzielle Überträger (vgl. *https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Steckbrief.html#doc13776792bodyText2*, Stand: 12.06.2020).

Ungeachtet dessen, dass Fieber grundsätzlich symptomatisch für eine SARS-CoV-2-Infektion sein kann, kann eine Temperaturmessung mit dem Ziel des Schutzes von Beschäftigten, Kunden oder Besuchern angesichts einer überwiegenden Anzahl symptomfreier Infektionsträger allenfalls als bedingt geeignet erachtet werden. Das RKI rät daher in seinem Epidemiologischen Bulletin 20/2020 vom 14.05.2020 von der Nutzung entsprechender Vorrichtungen an Flughäfen ab, da kein Mehrwert gesehen wird (*https://www.rki.de/DE/Content/Infekt/EpidBull/Archiv/2020/Ausgaben/20_20.pdf?__blob=publicationFile*).

In diesem Zusammenhang kommt daher der Prüfung besondere Bedeutung zu, ob mildere, weniger eingriffsintensive Maßnahmen zur Erreichung des verfolgten Zwecks, dem Schutz der Beschäftigten und Kunden, die gleichsam der Zweckerreichung dienen, ersichtlich sind. Angesichts dessen sind die üblichen Maßnahmen im **Einzelhandel**, wie etwa die Begrenzung der Kundenanzahl, das Anbringen von Hinweisschildern zu Verhaltensregeln und Zutrittsbeschränkungen, die Gewährleistung der Einhaltung von Mindestabständen, die Aufforderung zum Tragen eines Mundschutzes, die Anbringung von Trennwänden im Kassenbereich und an Verkaufstresen sowie die Implementierung von Hygienevorgaben zu nennen. Ein derartiges Maßnahmenpaket verspricht gerade auch im Hinblick auf die größere Gefahr der Virus-Exposition aufgrund nicht festgestellter symptomfrei Infizierter einen nachhaltigeren Schutz von Kunden und Beschäftigten als eine eingriffsintensive kameragestützte Erhebung von Gesundheitsdaten.

Im Ergebnis kann daher eine Erforderlichkeit der elektronischen Fiebermessung als Instrument der Zutrittsregulierung zu öffentlichen Verkaufs- und Verkehrsflächen, insbesondere im Bereich der Grundversorgung sowie für Bereiche, deren Nutzung für das tägliche Leben unabdingbar sind (z. B. Bahnhöfe, Flughäfen, Gebäude von Verwaltungsbehörden) nicht bejaht werden.

Bei der Fiebermessung als **betriebliche Maßnahme des Arbeitsschutzes** ist zu beachten, dass ihre rechtliche Zulässigkeit aufgrund der Konkretisierungsklausel des Art. 88 DSGVO anhand des § 26 BDSG zu beurteilen ist. Für Beschäftigte des öffentlichen Sektors der Länder ist das Personaldatenschutzrecht des jeweiligen Landes maßgeblich; auf dieses wird nachfolgend aber nicht weiter eingegangen. Im Hinblick auf die Erforderlichkeit ist zu berücksichtigen, dass der Verantwortliche als Arbeitgeber bzw. Dienstherr die Feststellung einer erhöhten Körpertemperatur mit nachfolgenden Untersuchungen kombinieren kann, was die Eignung der Maßnahme etwas erhöht. Nichtsdestotrotz ist im Hinblick auf die Erforderlichkeit zu berücksichtigen, dass symptomfreie Infektionsfälle durch eine elektronische Temperaturerfassung nicht aufgedeckt werden können. Im Übrigen bestünde – je nach Fragestellung und anlassbezogen – als mildere Maßnahme noch die Möglichkeit, nach gesundheitlichen Beeinträchtigungen der Arbeitsfähigkeit zu fragen, wenn dies wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt. Danach ist anlassbezogen die Frage nach dem Gesundheitszustand eines Beschäftigten zulässig, wenn gezielt die Beschäftigung unzumutbar machende potenzielle Ausfallzeiten oder Einschränkungen der Tätigkeit bestehen oder zu erwarten sind. Weiterhin darf allgemein nach dem Vorliegen von ansteckenden Krankheiten gefragt werden, die Kollegen oder Kunden gefährden könnten.

Bejaht man ungeachtet der vorstehenden Bedenken die Erforderlichkeit ebenso wie das Nichtüberwiegen der schutzwürdigen Interessen der betroffenen Personen, ist zu prüfen, ob das grundsätzliche Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO der Fiebermessung nicht entgegensteht. Nach den bereits gegebenen Hinweisen kommt insoweit gegenwärtig eine Ausnahme vom Verarbeitungsverbot nur noch nach Art. 9 Abs. 2 Buchstabe h DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 Buchst. b bzw. 26 Abs. 3 BDSG in Betracht. Danach ist eine Verarbeitung personenbezogener Gesundheitsdaten nicht verboten, wenn sie für die **Beurteilung der Arbeitsfähigkeit** erforderlich ist. Die Dokumentation müsste den zentralen Grundsätzen, u. a. der Zweckbindung, der Datenminimierung und Speicherbegrenzung, folgen. Zudem ist die Erfüllung der in Art. 9 Abs. 3 DSGVO, § 22 Absatz 1 Nummer 1 Buchstabe b) BDSG genannten Bedingungen und Garantien geboten. Mit anderen Worten dürfte eine elektronische Fiebermessung nur durch einen betriebsärztlichen Dienst vorgenommen werden. Dieser dürfte dem Arbeitgeber bzw. Dienstherrn allenfalls mitteilen, welchen Beschäftigten der Zutritt zum Betriebsgelände verweigert worden ist.

Im Bereich des betrieblichen Gesundheitsschutzes sind im Übrigen die Beteiligungsrechte der Interessenvertretungen zu beachten.

Die zulässige Verwendung elektronischer Temperaturmessgeräte hängt schließlich insgesamt von der Erfüllung **weiterer datenschutzrechtlicher Vorgaben** ab, z. B. sind die Regelungen zum Verzeichnis von Verarbeitungstätigkeiten, zur Datenschutz-Folgenabschätzung sowie zur Information nach Art. 12 ff. DSGVO (Hinweisbeschilderung) zu beachten.

Der Verantwortliche hat zudem dafür Sorge zu tragen, dass die Vorgaben des **Datenschutzes durch Technikgestaltung** aus Art. 25 DSGVO und der **Datensicherheit** nach Art. 32 DSGVO erfüllt werden. Hierbei können beispielsweise folgende Gesichtspunkte eine Rolle spielen:

– Geeignete Körperstellen zur Messung: Eine aussagekräftige Erfassung eines kompletten Wärmebilds eines Menschen ist kaum möglich, da z. B. die Kleidung die Infrarot-Abstrahlung verändern kann. In der Regel wird daher an der Stirn oder den Innenwinkeln der Augen gemessen. Es sind somit Spezialkameras nötig, die diese Stellen automatisiert erkennen und anvisieren können.
– Messgenauigkeit: Klassische kontaktlose Stirnthermometer haben häufig größere Abweichungen. Abhängig vom Einsatzkontext müssen daher Systeme zum Einsatz kommen, die eine deutlich höhere Messgenauigkeit haben, als übliche kontaktlose Fieberthermometer für den Hausgebrauch bieten.
– Verfälschung der Messung: Zudem muss berücksichtigt werden, dass neben anderen Erkrankungen auch körperliche Betätigung (Sport, Eile), Umgebungsbedingungen etc. zu Messunterschieden oder Abweichungen beitragen können.
– Absolute /relative Messung: Es gibt sowohl die Herangehensweise, einen Schwellwert festzulegen, ab dem die Wärmebildkamera positiv detektiert, als auch die Messung und Alarmierung im Vergleich zu den umgebenden Menschen durchzuführen. Im ersteren Fall stellt sich insbesondere die Schwierigkeit, wie der relevante Grenzwert für Fieber festzulegen ist, soweit die Körpertemperatur im Verlauf des Tages schwankt und zudem bei Kindern und Erwachsenen unterschiedlich ausfallen kann.
– Fehlerrate: Aufgrund der technischen Schwierigkeiten der Messung kann es auch unabhängig von der Problematik, dass Infizierte noch keine Symptome zeigen, zu „falsch-positiven“ wie auch „falsch-negativen“ Ergebnissen kommen, beispielsweise abhängig von der Festlegung der Schwellwerte und der Aufstellsituation.

– Auflösung, Bildgenauigkeit: Viele Wärmebildkameras bieten eine sehr hohe Auflösung, so dass sich die Frage stellt, welche zusätzlichen Informationen damit ersichtlich sind, insbesondere wenn ein Echtbild des Gesichts in hoher Auflösung erfasst wird (Erkennung anderer Krankheiten, biometrische Identifikation etc.).
– Automatische Messung /menschlicher Bediener: Aufgrund des Aufwands für die Messung ist davon auszugehen, dass diese nicht vollautomatisiert erfolgen kann, sondern zumindest von menschlichem Personal überwacht werden muss. Zudem ist im Fall einer positiven Detektion in der Regel menschliche Intervention nötig, um die betroffene Person herauszufiltern und weitere Maßnahmen zu ergreifen.

2.4
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12.05.2020

Zu Vorabwidersprüche bei StreetView und vergleichbaren Diensten

Für die Veröffentlichung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, die an den öffentlichen Straßenraum angrenzen, kann im Rahmen von Street-View und ähnlichen Diensten Art. 6 Abs. 1 Unterabsatz 1 lit. f DSGVO als Rechtsgrundlage in Betracht kommen. Dabei dürfen nur die personenbezogenen Daten veröffentlicht werden, die für die Zweckerreichung zwingend erforderlich sind; so sind Merkmale, die die Identifizierung einer Person ermöglichen, insbesondere Gesichter und KFZ-Kennzeichen, unkenntlich zu machen. Dies ergibt sich bereits aus Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung). Zudem hat der Anbieter vor Beginn der Aufnahmen die Öffentlichkeit in geeigneter Weise zu informieren.

Im Rahmen der Interessenabwägung ist ein Verlangen betroffener Personen auf Unkenntlichmachung personenbezogener Daten zu berücksichtigen. Dieses Verlangen kann zumindest ab dem Zeitpunkt der Anfertigung der Aufnahmen durch den Dienst wahrgenommen werden und umfasst auch Abbildungen von Häuserfassaden und privaten Grundstücksbereichen. Art. 21 DS-GVO bleibt unberührt.

Das Verlangen auf Unkenntlichmachung nach Art. 17 Abs. 1 DS-GVO und der Widerspruch nach Art. 21 DS-GVO müssen sowohl online als auch postalisch eingelegt werden können.

Auf diese Rechte muss ausdrücklich hingewiesen werden.

2.5
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12.05.2020

Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich

Google Analytics ist eines der weitest verbreiteten Tools für Website-Betreiber (Anwender). Mit Hilfe dieses Tools lassen sich umfassende statistische Auswertungen der Webseitennutzung vornehmen. Aus diesem Grund besteht ein großer Beratungsbedarf hinsichtlich des Einsatzes von Google Analytics.

Die Datenschutzaufsichtsbehörden haben vor dem Hintergrund des neuen Rechtsrahmens mit Geltung der DS-GVO den Einsatz von Google Analytics neu bewertet. Ältere Auffassungen der Datenschutzaufsichtsbehörden, die unter Berücksichtigung der Rechtslage vor dem 25.05.2018 kommuniziert wurden, gelten damit als überholt.[1]

Im Folgenden handelt es sich keinesfalls um eine abschließende Beurteilung. Die folgenden Ausführungen stellen eine Ergänzung der **Orientierungshilfe für Anbieter von Telemedien**[2] dar und betreffen lediglich die häufigsten Fragestellungen beim Einsatz von Google Analytics. Die folgenden Ausführungen stellen keine Empfehlung zum Einsatz von Google Analytics dar, sondern beschreiben nur die datenschutzrechtlichen **Mindestanforderungen**, die von Seitenbetreibern nach derzeitigem Stand zwingend eingehalten werden müssen.

Die Auffassungen der Datenschutzaufsichtsbehörden stehen unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss und der Rechtsprechung des EuGH.

Die Ausführungen gelten für den Fall, dass der Anwender von Google-Analytics die von Google derzeit[3] empfohlenen Standardeinstellungen nutzt. Für den Fall, dass der Anwender von Google Analytics von den empfohlenen Einstellungen abweicht und/oder ergänzende Funktionen verwendet (z. B. Google Analytics 360) oder Google die Verarbeitung oder die vertraglichen Grundlagen ändert, wird auf die von den deutschen Datenschutzaufsichts-

---

1 Dies gilt insbesondere für die Veröffentlichung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, „Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen".

2 Abrufbar unter: *https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf*

3 Stand: 11.03.2020

behörden veröffentlichten Ausführungen der Orientierungshilfe für Anbieter von Telemedien verwiesen.

I. Personenbezogene Daten

Beim Einsatz von Google Analytics werden immer personenbezogene Daten der Nutzer verarbeitet.

In den Google Analytics-Hilfen[4] erläutert Google, dass Nutzungsdaten keine „personenidentifizierbaren Informationen" seien. Diese Auffassung steht nicht nur im Widerspruch zur Definition des Begriffs „personenbezogene Daten" in Art. 4 Nr. 1 der DSGVO, sondern ist auch missverständlich, da Google im Weiteren Folgendes ausführt:

„Bitte beachten Sie, dass Daten, die Google nicht als personenidentifizierbare Informationen einstuft, im Rahmen der DS-GVO als personenbezogene Daten gelten können."

Die Datenschutzaufsichtsbehörden weisen daher ausdrücklich darauf hin, dass es sich bei den mit Google Analytics verarbeiteten Daten (Nutzungsdaten und sonstige gerätespezifische Daten, die einem bestimmten Nutzer zugeordnet werden können) um personenbezogene Daten i. S. d. DS-GVO handelt.

II. Verhältnis zwischen Google Analytics-Anwender und Google

Google hat die Verarbeitungsprozesse von Google Analytics fortlaufend angepasst. Dies hat dazu geführt, dass Google Analytics nicht mehr nur ein Tool zur statistischen Analyse (Reichweitenmessung) ist, sondern dem Anwender eine Vielzahl an weiteren Funktionen bietet, mit denen der Anwender verschiedene Zwecke verfolgen kann.

Nach Auffassung der Datenschutzaufsichtsbehörden ist die Verarbeitung im Zusammenhang mit Google Analytics keine Auftragsverarbeitung gemäß Art. 28 DS-GVO. Nach Art. 4 Nr. 7, Art. 28 Abs. 10 DS-GVO hat der Verantwortliche die Zwecke und Mittel der Verarbeitung selbst zu bestimmen. Daraus folgt die Pflicht des Auftragsverarbeiters, die Daten ausschließlich auf Weisung des Verantwortlichen zu verarbeiten (Art. 29 DS-GVO). Beim Einsatz von Google Analytics bestimmt der Website-Betreiber nicht allein über die Zwecke und Mittel der Datenverarbeitung. Diese werden vielmehr zum Teil ausschließlich von Google vorgegeben, so dass Google insoweit selbst verantwortlich ist, und vom Seitenbetreiber vertraglich akzeptiert. Die

4 Abrufbar unter der URL: *https://support.google.com/analytics/answer/7686480* [Stand: 27.09.2019].

Verarbeitung beim Einsatz von Google Analytics stellt einen einheitlichen Lebenssachverhalt dar, in dem die verschiedenen Aspekte der Verarbeitung nur als Ganzes einen Sinn ergeben. Dies hat zur Folge, dass die Beteiligten innerhalb einer Verarbeitungstätigkeit nicht ihre Rolle als Auftragsverarbeiter und/oder Verantwortlicher wechseln können.

Zwar bietet Google weiterhin einen Vertrag zur Auftragsverarbeitung an, stellt aber zusätzlich in den „Google Measurement Controller-Controller Data Protection Terms“[5] klar, dass für bestimmte Verarbeitungsprozesse Google und der Anwender (Website-Betreiber) getrennt verantwortlich seien. Zudem stellt Google in den Nutzungsbedingungen[6] klar, dass Google die Daten für eigene Zwecke, insbesondere auch zum Zweck der Bereitstellung seines Webanalyse- und Trackingdienstes, verarbeite. Gemäß Artikel 28 Abs. 10 DS-GVO handelt es sich bei Google damit nicht mehr um einen Auftragsverarbeiter.

Unter Berücksichtigung der aktuellen Rechtsprechung des EuGH sind Google und der Google-Analytics-Anwender gemeinsam für die Datenverarbeitung verantwortlich, so dass die Anforderungen des Art. 26 DS-GVO zu beachten sind.

III. Rechtsgrundlage

Der Einsatz von Google Analytics kann in aller Regel nicht auf Art. 6 Abs. 1 lit. b DS-GVO gestützt werden, da der Einsatz von Google Analytics nicht zur Vertragserfüllung zwischen Website-Betreiber und Nutzer erforderlich ist.

Der Einsatz von Google Analytics ist *in der Regel* auch nicht nach Art. 6 Abs. 1 lit. f DSGVO rechtmäßig. Angesichts der konkreten Datenverarbeitungsschritte beim Einsatz von Google Analytics überwiegen die Interessen, Grundrechte und Grundfreiheiten der Nutzer regelmäßig die Interessen der Website-Betreiber. Insbesondere rechnet der Nutzer vernünftigerweise nicht damit, dass seine personenbezogenen Daten mit dem Ziel der Erstellung personenbezogener Werbung und der Verknüpfung mit den aus anderen Zusammenhängen gewonnenen personenbezogenen Daten an Dritte weitergegeben und umfassend ausgewertet werden.[7] Dies geht weit über das

---

5 Das „Google Measurement Controller-Controller Data Protection Terms“, abrufbar unter: *https://support.google.com/analytics/answer/9012600*, Fassung vom 4. November 2019, Ziff. 4, gilt u. a. für den Fall, dass Google-Produkte und -Dienste in den Einstellungen zur Datenfreigabe aktiviert sind.

6 Abrufbar unter: *https://marketingplatform.google.com/about/analytics/terms/de/*, Fassung vom 17. Juni 2019, Ziff. 6, 7.

7 Datenschutzerklärung von Google unter: *https://policies.google.com/privacy*, Fassung wirksam ab dem 15. Oktober 2019, unter der Überschrift „Messung der Leistung“.

hinaus, was im Rahmen des Art. 6 Abs. 1 lit. f DS-GVO zulässig ist.[8] Die Situation weicht insoweit erheblich von dem Fall einer Statistikfunktion auf der eigenen Website oder mittels Auftragsverarbeitung ab.

Google verpflichtet in den vertraglichen Regelungen den Anwender von Google Analytics, unter bestimmten Voraussetzungen für den Einsatz des Dienstes eine Einwilligung der Besucher der Webseite einzuholen.[9] Die Datenschutzaufsichtsbehörden weisen ausdrücklich darauf hin, dass es für den rechtmäßigen Einsatz von Google Analytics nicht auf die vertraglichen Vereinbarungen zwischen Google und dem Anwender ankommt. Die Rechtmäßigkeit richtet sich ausschließlich nach dem Gesetz.

Im Ergebnis ist ein rechtmäßiger Einsatz von Google Analytics in der Regel nur aufgrund einer wirksamen Einwilligung der Webseitenbesuchenden gem. Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO möglich.

IV. Maßnahmen

Sofern Website-Betreiber nicht auf alternative und datensparsame Werkzeuge zur Reichweitenmessung ausweichen, sondern weiterhin Google Analytics verwenden, sind insbesondere folgende Maßnahmen umzusetzen:

1) Einholung einer informierten, freiwilligen, aktiven und vorherigen Einwilligung der Nutzer

Eine Einwilligung ist nur wirksam, wenn die Anforderungen gem. Art. 4 Nr. 11, Art. 7 DSGVO und ggf. Art. 8 DS-GVO erfüllt sind. Das bedeutet insbesondere:

– Website-Betreiber müssen sicherstellen, dass die Einwilligung die **konkrete Verarbeitungstätigkeit** durch die Einbindung von Google Analytics und damit verbundene Übermittlungen des Nutzungsverhaltens an Google LLC erfasst.
– In der Einwilligung muss **klar und deutlich** beschrieben werden, dass die Datenverarbeitung im Wesentlichen durch Google erfolgt, die Daten nicht anonym sind, welche Daten verarbeitet werden und dass Google diese zu

8 Nähere Erläuterungen in der „Orientierungshilfe für Anbieter von Telemedien".

9 Vgl. „**Nutzungsbedingungen"**, abrufbar unter: https://marketingplatform.google.com/about/analytics/terms/de/, Fassung vom 17. Juni 2019; „**Richtlinienanforderungen für Google Analytics-Werbefunktionen**", abrufbar unter: *https://support.google.com/analytics/answer/2700409*, Fassung vom 16. Dezember 2016; „**Richtlinie zur Einwilligung der Nutzer in der EU**", abrufbar unter: *https://www.google.com/about/company/user-consentpolicy.html*, ohne Datum, zuletzt abgerufen am 23. Januar 2020.

beliebigen eigenen Zwecken wie zur Profilbildung nutzt sowie mit anderen Daten wie eventuellen Google-Accounts verknüpft. Ein bloßer Hinweis wie z. B. „diese Seite verwendet Cookies, um Ihr Surferlebnis zu verbessern“ oder „verwendet Cookies für Webanalyse und Werbemaßnahmen“ ist nicht ausreichend, sondern irreführend, weil die damit verbundenen Verarbeitungen nicht transparent gemacht werden.

– Nutzer müssen **aktiv** einwilligen, d. h. die Zustimmung darf nicht unterstellt und ohne Zutun des Nutzers voreingestellt sein. Ein Opt-Out-Verfahren reicht nicht aus, vielmehr muss der Nutzer durch aktives Tun (z. B. Anklicken eines Buttons) seine Zustimmung zum Ausdruck bringen. Google muss ausdrücklich als Empfänger der Daten aufgeführt werden. Vor einer aktiven Einwilligung des Nutzers dürfen keine Daten erhoben oder Elemente von Google-Websites nachgeladen werden. Auch das bloße Nutzen einer Website (oder einer App) stellt keine wirksame Einwilligung dar.
– **Freiwillig** ist die Einwilligung nur, wenn die betroffene Person Wahlmöglichkeiten und eine freie Wahl hat. Sie muss eine Einwilligung auch verweigern können, ohne dadurch Nachteile zu erleiden. Die Koppelung einer vertraglichen Dienstleistung an die Einwilligung zu einer für die Vertragserbringung nicht erforderlichen Datenverarbeitung kann gemäß Art. 7 Abs. 4 DS-GVO dazu führen, dass die Einwilligung nicht freiwillig und damit unwirksam ist.

Um die Anforderungen einer wirksamen Einwilligung auf Websites oder in Apps umzusetzen, sind folgende Gestaltungshinweise zu beachten:

– **Klare, nicht irreführende Überschrift** – bloße „Respektbekundungen“ bezüglich der Privatsphäre reichen nicht aus. Es empfehlen sich Überschriften, in denen auf die Tragweite der Entscheidung eingegangen wird, wie beispielsweise *„Datenverarbeitung Ihrer Nutzerdaten durch Google“*.
– **Links** müssen **eindeutig** und unmissverständlich beschrieben sein – wesentliche Elemente/Inhalte insbesondere einer Datenschutzerklärung dürfen nicht durch Links verschleiert werden.
– Der **Gegenstand** der Einwilligung muss **deutlich gemacht** werden: Anwender von Google Analytics müssen deutlich machen, für welchen Zweck Google Analytics verwendet wird, dass die Nutzungsdaten von Google LLC verarbeitet werden, diese Daten in den USA gespeichert werden, sowohl Google als auch staatliche Behörden Zugriff auf diese Daten haben, diese Daten mit anderen Daten des Nutzers wie beispielsweise dem Suchverlauf, persönlichen Accounts, den Nutzungsdaten anderer Geräte und allen anderen Daten, die Google zu diesem Nutzer vorliegen, verknüpft werden.

– Der **Zugriff auf das Impressum und die Datenschutzerklärung** darf nicht verhindert oder eingeschränkt werden.

2) Technische Anforderungen an die Umsetzung des Widerrufs der Einwilligung

Beim Einsatz von Google Analytics muss stets ein einfach und immer zugänglicher Mechanismus (z. B. Schaltfläche) zum Widerruf der einmal vom Nutzer erteilten Einwilligung implementiert sein. Gleiches gilt für Apps, die zum Beginn der Nutzung eine Einwilligung erfragen. Auch hier muss in den Einstellungen eine einfach zugängliche Möglichkeit zum wirksamen Widerruf der Einwilligung vorhanden sein.

Hatte ein Nutzer einmal seine Einwilligung erteilt und widerruft er sie zu einem späteren Zeitpunkt, so ist sicherzustellen, dass nach dem Widerruf das Google Analytics-Skript nicht nachgeladen oder ausgeführt wird.

Google stellt ein Browser-Add-On zur Deaktivierung von Google Analytics zur Verfügung. Es ist nicht zulässig, den Nutzer ausschließlich auf dieses Add-On zu verweisen, da dies keine hinreichende Widerrufsmöglichkeit darstellt. Gemäß Art. 7 Abs. 3 S. 4 DS-GVO ist der Widerruf so einfach wie die Erteilung der Einwilligung zu gestalten. Das von Google zur Verfügung gestellte Add-On erfüllt diese Anforderungen nicht, da der Nutzer zum

Herunterladen von weiteren Programmen gezwungen wird. Im Übrigen entspricht das AddOn aufgrund der Vielzahl an Browsern und Betriebssystemen weder dem Stand der Technik noch ist es geeignet, um die Datenverarbeitung in Apps zu unterbinden.

3) Transparenz

Anwender müssen gemäß Art. 13 DS-GVO die Nutzer in den Datenschutzbestimmungen umfassend über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics informieren. Bezüglich der Anforderungen an diese Informationspflicht wird auf die **Leitlinie zur Transparenz**[10] des Europäischen Datenschutzausschusses sowie auf die **Orientierungshilfe für Anbieter von Telemedien** verwiesen.

10 Abrufbar unter: *https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_rev01.docx*

4) Kürzung der IP-Adresse

Zusätzlich zu den o. g. Maßnahmen sollten Anwender von Google Analytics durch entsprechende Einstellungen die Kürzung der IP-Adressen veranlassen. Dazu ist auf jeder Internetseite mit einer Google Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()“ zu ergänzen. Weitere Details können der technischen Anleitung von Google entnommen werden, abrufbar unter: https://developers.google.com/analytics/devguides/collection/gtagjs/ip-anonymization.

Die Kürzung der IP-Adresse stellt eine zusätzliche Maßnahme gem. Art. 25 Abs. 1 DS-GVO zum Schutz der Nutzer dar, sie führt jedoch nicht dazu, dass die vollständige Datenverarbeitung anonymisiert erfolgt. Beim Einsatz von Google Analytics werden neben der IP-Adresse weitere Nutzungsdaten erhoben, die als personenbezogene Daten zu bewerten sind, wie z. B. Identifizierungsmerkmale der einzelnen Nutzer, die auch eine Verknüpfung beispielsweise mit einem vorhandenen Google-Account erlauben. Aus diesem Grund ist in jedem Fall der Anwendungsbereich der DS-GVO eröffnet, so dass Anwender von Google Analytics auch dann verpflichtet sind, die Anforderungen der DS-GVO zu beachten, wenn sie die Kürzung der IP-Adressen veranlasst haben. In der Datenschutzerklärung ist der Umstand, ob die Kürzung der IP-Adressen veranlasst ist, entsprechend anzugeben.

Im Übrigen gelten die Ausführungen der Orientierungshilfe für Anbieter von Telemedien.

2.6
Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 15.04.2020

Zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung

Aus Sicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestehen gegen den bundesweiten Einsatz der Einwilligungsdokumente der Medizininformatik-Initiative in der Version 1.6b, bestehend aus einer Patienteninformation und einer Einwilligungserklärung sowie der zugehörigen Handreichung in der Version 0.9b keine Bedenken, unter der Voraussetzung, dass in den Einwilligungsdokumenten auf die Verarbeitung genetischer Daten aus Biomaterialien und insbesondere das damit verbun-

dene Risiko der Rückverfolgbarkeit explizit hingewiesen wird, die Wahrung des jederzeitigen Widerrufsrechts trotz der Übertragung des Eigentums an Biomaterialien klarer zum Ausdruck kommt und Patienten auf die Möglichkeit hingewiesen werden, sich bei einem E-Mail-Verteiler zu registrieren, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert. In der Handreichung ist außerdem die Passage zu streichen, in der darauf hingewiesen wird, dass zukünftig die Datenübermittlung in Drittstaaten zulässig sein soll.

Zur Umsetzung dieser Anforderungen in der Patienteninformation wird vorgeschlagen:

– Unter 3.2 im ersten Absatz nach Satz 2 einzufügen: „In Biomaterialien kann Ihre Erbsubstanz in Form genetischer Daten enthalten sein. Insofern sind insbesondere die unter 1.4 beschriebenen Risiken für genetische Daten zu beachten. Hierzu zählt auch ein erhöhtes Risiko einer Rückverfolgbarkeit Ihrer Person anhand dieser Daten."
– Unter 3.3 im ersten Absatz nach Satz 2 einzufügen: „Ihr Recht, über die Verarbeitung Ihrer personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsübertragung unberührt. Trotz Eigentumsübertragung können Sie Ihre Einwilligung in die Datenverarbeitung jederzeit widerrufen (siehe Punkt 6) und die Vernichtung Ihrer Biomaterialien verlangen."
– Zudem ist in der Einwilligung und in der Patienteninformation jeweils an geeigneter Stelle auf die Möglichkeit der Registrierung bei einem E-Mail-Verteiler hinzuweisen, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert.

Ergänzend sollte in der Einwilligungserklärung in dem Kasten unter 3.3 als zweiter Satz aufgenommen werden: „Mein Recht, über die Verarbeitung meiner dem Biomaterial zu entnehmenden personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsübertragung unberührt (siehe Punkt 3.3 der Patienteninformation)."

Als redaktionelle Korrektur wird zudem empfohlen, in der Einwilligungserklärung unter 1.1 zum Stichwort der Codierung auch auf Punkt 1.3 der Patienteninformation zu verweisen, da die Codierung dort beschrieben wird.

3. Ausgewählte Orientierungshilfen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

3.1
Orientierungshilfe des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ – 13.03.2020

Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail[11]

1. Zielstellung

Die vorliegende Orientierungshilfe zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter[12] auf dem Transportweg zu erfüllen sind. Diese Anforderungen richten sich nach den Vorgaben des Art. 5 Abs. 1 lit. f, 25 und 32 Abs. 1 DS-GVO. Die Orientierungshilfe nimmt den Stand der Technik zum Veröffentlichungszeitpunkt als Ausgangspunkt für die Konkretisierung der Anforderungen.

Verantwortliche und Auftragsverarbeiter[13] sind gesetzlich gehalten, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, hinreichend zu mindern. Sie müssen hierbei Art, Umfang, Umstände und Zwecke ihrer Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Diese Orientierungshilfe behandelt ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind. Sie setzt voraus, dass die Verantwortlichen bzw. ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können.

Die Orientierungshilfe geht von typischen Verarbeitungssituationen aus. Sie bestimmt hierbei ausgehend vom Stand der Technik, den typischen Implementierungskosten und deren Verhältnis zu den Risiken einer Übermittlung personenbezogener Daten per E-Mail Anforderungen an die Maßnahmen, die Verantwortliche und Auftragsverarbeiter zur ausreichenden Minderung

11 Die Orientierungshilfe wurde durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder gegen die Stimme Bayerns beschlossen.

12 Diensteanbieter, die eigene oder fremde E-Mail-Dienste zur öffentlichen Nutzung bereithalten.

13 Auftragsverarbeiter ausschließlich im Hinblick auf ihre Pflichten nach Art. 32 DS-GVO.

der Risiken zu treffen haben. Die Verantwortlichen und Auftragsverarbeiter sind verpflichtet, die Besonderheiten ihrer Verarbeitungen, darunter insbesondere den Umfang, die Umstände und die Zwecke der vorgesehenen Übermittlungsvorgänge zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können. Dabei müssen sie berücksichtigen, dass die vorliegende Orientierungshilfe ausschließlich Risiken betrachtet, die sich auf dem Transportweg ergeben. Risiken, denen ruhende Daten wie bereits empfangene E-Mails ausgesetzt sind oder die durch eine Weiterverarbeitung wie z. B. automatische Weiterleitungen entstehen, werden in dieser Orientierungshilfe nicht betrachtet und können weitere Maßnahmen oder eine andere Gewichtung der im Folgenden aufgeführten Maßnahmen notwendig machen. Können die Anforderungen an eine sichere Übermittlung per E-Mail nicht erfüllt werden, so muss ein anderer Kommunikationskanal gewählt werden.[14]

2. Anwendungsbereich und Grundsätze

Der gesetzlich gebotene Schutz personenbezogener Daten im Zuge der Übermittlung von E-Mail-Nachrichten erstreckt sich sowohl auf die personenbezogenen Inhalte als auch die Umstände der Kommunikation, soweit sich aus letzteren Informationen über natürliche Personen ableiten lassen.[15] Dieser Schutz muss abseits des Blickwinkels dieser Orientierungshilfe ergänzt werden durch Maßnahmen zum Schutz der beteiligten Systeme und zur Minimierung, Speicherbegrenzung und Zweckbindung der auf diesen Servern verarbeiteten Verkehrsdaten.

Diese Orientierungshilfe thematisiert den Vertraulichkeitsschutz der personenbezogenen Inhalte der E-Mail-Nachrichten lediglich insoweit, wie diese nicht bereits vorab (z. B. anwendungsspezifisch) gemäß dem Stand der Technik so verschlüsselt wurden, dass nur der Empfänger sie entschlüsseln kann.

Sowohl Ende-zu-Ende-Verschlüsselung als auch Transportverschlüsselung mindern für ihren jeweiligen Anwendungszweck Risiken für die Vertraulichkeit der übertragenen Nachrichten. Daher müssen Verantwortliche beide Verfahren in der Abwägung der notwendigen Maßnahmen berücksichtigen.

---

14 Für die Kommunikation mit betroffenen natürlichen Personen (z. B. mit Kunden) kann ein Kommunikationsweg in der Bereitstellung eines Webportals bestehen.

15 Informationen über die Umstände der Kommunikation lassen sich verschiedenen Verarbeitungsprozessen entnehmen, die mit Versand und Empfang von E-Mail-Nachrichten in Verbindung stehen (vom Abruf von Angaben aus dem DNS bis zur Protokollierung der Kommunikation auf verschiedenen Geräten). Diese Orientierungshilfe thematisiert lediglich den Schutz der in den Kopfzeilen einer E-Mail-Nachricht enthaltenen Angaben während des Transports der Nachricht.

Der durchgreifendste Schutz der Vertraulichkeit der Inhaltsdaten wird durch Ende-zu-Ende-Verschlüsselung erreicht, wofür derzeit die Internet-Standards S/MIME (RFC 5751) und OpenPGP (RFC 4880) i. d. R. in Verbindung mit PGP/MIME (RFC 3156) zur Verfügung stehen. Ende-zu-Ende-Verschlüsselung schützt nicht nur den Transportweg, sondern auch ruhende Daten. Bei Ende-zu-Ende-Verschlüsselung kann die Verarbeitung unverschlüsselter Inhaltsdaten auf besonders geschützte Netzsegmente bzw. auf solche Teile des Netzes beschränkt werden, die ausschließlich zur Nutzung durch Befugte (wie eine Personalabteilung oder einen Amtsarzt) vorgesehen sind.

Der Einsatz von Transportverschlüsselung bietet einen Basisschutz und stellt eine Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen dar. In Verarbeitungssituationen mit normalen Risiken wird dabei bereits durch die Transportverschlüsselung eine ausreichende Risikominderung erreicht.

Die Transportverschlüsselung reduziert die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß. Um auch gegen Dritte zu bestehen, die aktiv in den Netzverkehr eingreifen, muss sie in qualifizierter Weise durchgeführt und durch Maßnahmen zur kryptografischen Absicherung der Angaben der Empfänger über die zur Entgegennahme der Nachrichten berechtigten Geräte flankiert werden.

Eine Darstellung der Anforderungen an die einfache und an die qualifizierte obligatorische Transportverschlüsselung sowie an die Ende-zu-Ende-Verschlüsselung und die Signatur von E-Mail-Nachrichten ist in Abschnitt 5 niedergelegt.

3. Die Inanspruchnahme von E-Mail-Diensteanbietern

3.1 *Grundlegende technische Anforderungen an die Erbringung von E-Mail-Diensten*

Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der TR 03108-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten.

Dies bedeutet, dass sie verpflichtend die in dieser Technischen Richtlinie niedergelegten Voraussetzungen für einen geschützten Empfang von Nachrichten schaffen und bei dem Versand von Nachrichten in Bezug auf die Anwendung von kryptografischen Algorithmen und die Überprüfung der Authentizität und Autorisierung der Gegenstelle den unter den gegebenen Bedingungen auf Empfängerseite bestmöglichen mit verhältnismäßigen Mitteln erreichbaren Schutz erzielen müssen.

3.2 Sorgfaltspflicht bei der Inanspruchnahme von E-Mail-Diensteanbietern

Verantwortliche, die öffentliche E-Mail-Diensteanbieter in Anspruch nehmen, müssen sich davon überzeugen, dass die Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DSGVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung eigener Systeme und Endgeräte an die Diensteanbieter ein.

Darüber hinaus müssen die Verantwortlichen die Risiken sorgfältig einschätzen, die mit dem Bruch der Vertraulichkeit und Integrität von E-Mail-Nachrichten verbunden sind, die sie versenden oder gezielt empfangen. In Abhängigkeit von diesen Risiken können sich die im Folgenden dargestellten zusätzlichen Anforderungen ergeben, deren Erfüllung sie durch Weisung an den Diensteanbieter (z. B. durch Vornahme geeigneter Konfigurationseinstellungen, soweit solche von dem Diensteanbieter angeboten werden) durchsetzen müssen.

4. Fallgruppen

4.1 Gezielte Entgegennahme von personenbezogenen Daten in den Inhalten von E-Mail-Nachrichten

Verantwortliche, die gezielt personenbezogene Daten per E-Mail entgegennehmen, z. B. durch explizite Vereinbarung des Austauschs personenbezogener Daten per E-Mail oder die Aufforderung auf der Homepage, personenbezogene Daten per E-Mail zu übermitteln, haben die im Folgenden beschriebenen Verpflichtungen zu erfüllen.

4.1.1 Verpflichtungen bei normalen Risiken[16]

Der Schutz von Vertraulichkeit und Integrität von personenbezogenen Daten bei der Übermittlung von E-Mail-Nachrichten setzt voraus, dass Sender und Empfänger zusammenarbeiten. Die Verantwortung für den einzelnen Übermittlungsvorgang liegt bei dem Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen (direkt per SMTPS oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss und hierbei ausschließlich

16 Zur Einstufung von Risiken s. das Kurzpapier Nr. 18 der unabhängigen Datenschutzbehörden des Bundes und der Länder „Risiko für die Rechte und Freiheiten natürlicher Personen“, abrufbar unter *https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/kurzpapiere/DSK_KPNr_18_Risiko.pdf.*

die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf. Um den Aufbau verschlüsselter Verbindungen zu erleichtern, sollte der Verantwortliche für Verschlüsselung und Authentifizierung ein möglichst breites Spektrum an qualifizierten Algorithmen anbieten.

Um die Authentizität und Integrität der empfangenen E-Mail-Nachrichten zu überprüfen, sollten Verantwortliche DKIM-Signaturen prüfen und signierte Nachrichten, bei denen die Prüfung fehlschlägt, markieren oder, bei entsprechender Festlegung des Absenders über einen DMARC-Eintrag im DNS, zurückweisen.

4.1.2 Verpflichtungen bei hohen Risiken

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte Transportverschlüsselung (s. u. Nr. 5.2) als auch den Empfang von Ende-zu-Ende-verschlüsselten Nachrichten ermöglichen.

Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen (s. u. Nr. 5.4).

4.2 Versand von E-Mail-Nachrichten

4.2.1 Verpflichtungen bei normalen Risiken

Alle Verantwortlichen, die E-Mail-Nachrichten mit personenbezogenen Daten versenden, bei denen ein Bruch der Vertraulichkeit (des Inhalts oder Umstände der Kommunikation, soweit sie sich auf natürliche Personen beziehen) ein Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, sollten sich an der TR 03108-1 orientieren und müssen eine obligatorische Transportverschlüsselung sicherstellen.

4.2.2 Versand von E-Mail-Nachrichten bei hohem Risiko

Verantwortliche, die E-Mail-Nachrichten versenden, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellt, müssen regelmäßig eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung vornehmen. Inwieweit entweder auf die Ende-zu-Ende-Verschlüsselung oder die Erfüllung einzelner Anforderungen an diese (s. Kap. Ende-zu-Ende-Verschlüsselung) oder an die qualifizierte

Transportverschlüsselung (z. B. DANE oder DNSSEC) verzichtet werden kann, hängt von den bestehenden Risiken, der konkreten Ausgestaltung des Übertragungsweges und ggf. getroffenen kompensierenden Maßnahmen ab.

4.2.3 Versand von E-Mail-Nachrichten mit geheim zu haltenden Inhalten bei hohen Risiken

Verantwortliche, die aufgrund von § 203 StGB zur Geheimhaltung von Kommunikationsinhalten verpflichtet sind, müssen über die unter 4.2.1 bzw. 4.2.2 aufgeführten Anforderungen hinaus durch Verschlüsselung sicherstellen, dass nur Stellen eine Entschlüsselung vornehmen können, an die die Inhalte der Nachrichten offenbart werden dürfen.

5. Anforderungen an die Verschlüsselungs- und Signaturverfahren

5.1 Obligatorische Transportverschlüsselung

Durch eine obligatorische Transportverschlüsselung soll eine unverschlüsselte Übermittlung der Nachrichten ausgeschlossen werden. Sie kann über das Protokoll SMTPS oder durch Aufruf des SMTP-Befehls STARTTLS und den nachfolgenden Aufbau eines mit dem Protokoll TLS verschlüsselten Kommunikationskanals realisiert werden, wobei die Anforderungen der TR 02102-2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen sind.

Bei dem letztgenannten Verfahren (STARTTLS) kann die obligatorische Transportverschlüsselung durch entsprechende Konfiguration des sendenden MTA (Mail Transfer Agent) erreicht werden; die entsprechenden Konfigurationseinstellungen werden (En)Forced TLS, Mandatory TLS o. ä. genannt. Unterstützt die Gegenstelle kein TLS, dann wird der Verbindungsaufbau abgebrochen. Einige MTA ermöglichen eine domänenspezifische oder regelbasierte Spezifizierung dieses Verhaltens.

5.2 Qualifizierte Transportverschlüsselung

Transportverschlüsselung erreicht unter folgenden Voraussetzungen einen ausreichenden Schutz gegen aktive Angriffe von Dritten, die in der Lage sind, den Netzwerkverkehr auf der Übermittlungsstrecke zu manipulieren:

1. Die eingesetzten kryptografischen Algorithmen und Protokolle entsprechen dem Stand der Technik: Sie erfüllen die Anforderungen der Technischen Richtlinie BSI TR-02102-2 und garantieren Perfect Forward Secrecy.
2. Die Bezeichnung der zum Empfang autorisierten Mailserver und ihre IP-Adressen wurden auf Empfängerseite per DNSSEC signiert. Die Si-

gnaturen der DNS-Einträge werden auf Senderseite überprüft. Alternativ kann die Bezeichnung der zum Empfang autorisierten Mailserver auch durch Kommunikation mit dem Empfänger verifiziert werden.

3. Der empfangende Server wird im Zuge des Aufbaus der verschlüsselten Verbindung entweder zertifikatsbasiert authentifiziert oder anhand eines öffentlichen oder geheimen Schlüssels, der über einen anderen Kanal zwischen Sender und Empfänger abgestimmt wurde.
4. Erfolgt die Authentifizierung zertifikatsbasiert, so führt der Empfänger die Authentizität des Zertifikats auf ein vertrauenswürdiges Wurzelzertifikat bzw. einen via DANE publizierten Vertrauensanker zurück.

Die Einhaltung dieser Anforderungen muss nachgewiesen werden.

5.3 Ende-zu-Ende-Verschlüsselung

Durch eine Ende-zu-Ende-Verschlüsselung mit den Verfahren S/MIME und OpenPGP ist es möglich, die Inhalte einer E-Mail-Nachricht durchgreifend gegen unbefugte Kenntnisnahme zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

1. Der Verantwortliche muss die öffentlichen Schlüssel der Empfänger auf die Einhaltung hinreichender Sicherheitsparameter (insbesondere einer hinreichenden Schlüssellänge) überprüfen, sie durch Verifikation der Zertifikate bzw. Beglaubigungen authentisieren, vor jedem Versand bzw. Signaturprüfung auf Gültigkeit überprüfen und zuverlässig verwalten.
2. Die Überprüfung der Authentizität eines Schlüssels kann regelmäßig durch Verifikation eines Zertifikats eines vertrauenswürdigen Zertifikatsdienstanbieters (S/MIME) oder Beglaubigung anderer vertrauenswürdiger und nachweislich zuverlässiger Dritter (OpenPGP) erfolgen. Es sei ausdrücklich darauf hingewiesen, dass die Veröffentlichung eines Schlüssels auf einem OpenPGP-Schlüsselserver kein Indiz für die Authentizität dieses Schlüssels ist. Die Überprüfung des Fingerprints eines OpenPGP-Keys ist für die Überprüfung der Authentizität eines Schlüssels ausreichend, sofern der Fingerprint mit einer sicheren kryptografischen Hashfunktion (s. BSI TR-02102) ermittelt und die Authentizität des Vergleichswerts z. B. durch direkte Kommunikation mit dem Empfänger über einen anderen Kanal überprüft wurde.
3. Die Authentizität eines über Web Key Directory (WKD) bereitgestellten öffentlichen Schlüssels ist äquivalent zu der Authentizität des bereit-

stellenden Webservers. Für die Überprüfung gelten die Anforderungen an die Überprüfung der Authentizität des empfangenden Mailservers entsprechend.

4. Diese Anforderung kann auch nachträglich in Bezug auf Schlüssel erfüllt werden, die zunächst opportunistisch ausgetauscht wurden (z. B. per Autocrypt). Hierzu ist eine Verifikation der Authentizität über einen anderen Kanal erforderlich.
5. Die Überprüfung der Gültigkeit eines S/MIME-Schlüssels vor seinem Einsatz soll durch Abruf von Gültigkeitsinformationen bei dem Zertifikatsdiensteanbieter (Abruf von CRL via http, OCSP) erfolgen. Die Überprüfung der Gültigkeit eines OpenPGP-Schlüssels ist nur möglich, wenn der Eigner bekannt gegeben hat, wo er ggf. Revokationszertifikate zu veröffentlichen beabsichtigt. Dies kann z. B. ein OpenPGP-Schlüsselserver oder die Webseite des Schlüsseleigners sein. Sofern es an einer solchen Abrufmöglichkeit fehlt, müssen Garantien dafür bestehen, dass alle Nutzer eines Schlüssels unverzüglich informiert werden, wenn dieser seine Gültigkeit – insbesondere aufgrund einer Kompromittierung des zugehörigen privaten Schlüssels – verliert.

Wer Nachrichten Ende-zu-Ende-verschlüsselt, sollte beachten, dass Perfect Forward Secrecy durch Ende-zu-Ende-Verschlüsselung allein nicht gegeben ist, so dass eine Kompromittierung des privaten Schlüssels eines Empfängers alle Nachrichten gefährdet, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden. E-Mail-Nachrichten, die von Dritten abgefangen werden, können von diesen aufbewahrt und bei Offenlegung des privaten Schlüssels eines der Empfänger zu einem späteren Zeitpunkt entschlüsselt werden.

5.4 Signatur

Durch eine Signatur mit den Verfahren S/MIME und OpenPGP ist es möglich, die Integrität der Inhalte einer E-Mail-Nachricht nachhaltig gegen unbefugte Beeinträchtigung zu schützen. Dieser Schutz erstreckt sich dabei nicht nur auf den eigentlichen Transportweg, sondern auch auf die Zwischenspeicherung und -verarbeitung auf den an der Übermittlung beteiligten Servern. Um diese Wirksamkeit zu erreichen, sind folgende Voraussetzungen einzuhalten:

Sender müssen die eigenen Signaturschlüssel mit hinreichenden Sicherheitsparametern erzeugen sowie die privaten Schlüssel sicher speichern und nutzen, und sie müssen, soweit kein direkter Abgleich der Schlüssel zwischen Sender und Empfänger stattfindet, die korrespondierenden öffentlichen Schlüssel von zuverlässigen und vertrauenswürdigen Dritten zertifizieren lassen und sie ihren Kommunikationspartnern zur Verfügung stellen. Emp-

fänger sollen in Abhängigkeit von den Authentizitäts- und Integritätsrisiken die in Kap. Ende-zu-Ende-Verschlüsselung aufgeführten Maßnahmen auf die Überprüfung und das Management der Schlüssel der Sender in entsprechender Weise anwenden.

II
Zweiter Teil
3. Tätigkeitsbericht zur Informationsfreiheit

1. Einführung Informationsfreiheit

Die Informationsfreiheit läuft erst allmählich an. Die Zahl der geltend gemachten Informationsansprüche hält sich noch in Grenzen. Auch haben die Kommunen von der Möglichkeit, eigene Informationsfreiheitsordnungen zu schaffen, noch kaum Gebrauch gemacht. Auf diese Entwicklung habe ich als Vorsitzender der Informationsfreiheitskonferenz im Berichtsjahr aufmerksam gemacht und sah darin eine Bestätigung des hessischen Modells, welches Datenschutz und Informationsfreiheit verklammert und in einen sinnvollen Zusammenhang bringt. Dieses bewährte sich auch im Zusammenhang der Corona-Pandemie, die aufzeigte, dass nicht die Quantität der Informationen entscheidend ist, sondern deren Gehalt und Qualität.

2. Unangemessener Ausschluss der Informationsfreiheit gegenüber dem Landesamt für Verfassungsschutz und gegenüber Polizeibehörden

Es ist sowohl aus Gründen der Informationsfreiheit als auch mit Blick auf die Aufgabenstellung von Polizeibehörden und dem Landesamt für Verfassungsschutz unangemessen, Informationsfreiheitsansprüche gegenüber diesen Stellen gänzlich auszuschließen. Soweit die Wahrnehmung der Aufgaben dieser Stellen nicht beeinträchtigt wird, ist es geboten, Informationsfreiheit zu gewährleisten.

Im vergangenen Jahr 2020 hatte ich den Vorsitz der Konferenzen der Informationsfreiheitsbeauftragten von Bund und Ländern (IFK) inne. Ein Gegenstand der Erörterungen war der Informationszugang in Bund und Ländern gegenüber dem Verfassungsschutz sowie der Polizei. Es stellte sich leider heraus, dass Hessen in diesem Punkt nicht „vorne“, sondern eher „hinten“ liegt.

Das liegt daran, dass Hessen gegenüber diesen Behörden jegliche Informationsfreiheit ausschließt, § 81 Abs. 2 Nr. 1 HDSIG, indem die Anwendung der informationsfreiheitsrechtlichen hessischen Regelungen auf diese Behörden gesetzlich negiert ist.

§ 81 HDSIG
(…)
(2) Die Vorschriften des Vierten Teils gelten nicht für
1. die Polizeibehörden und das Landesamt für Verfassungsschutz
(…)

Aufgabenstellung des Verfassungsschutzes und der Polizei

Die Ämter für Verfassungsschutz haben die Aufgabe, Informationen über verfassungsfeindliche Bestrebungen, die gegen die freiheitlich demokratische Grundordnung, gegen den Bestand oder die Sicherheit von Bund oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung des Bundes oder eines Landes zum Ziel haben, zu sammeln und auszuwerten. Weitere Aufgabenfelder sind insbesondere Spionageabwehr, also die Bekämpfung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten anderer Staaten, sowie die Beobachtung von Gruppierungen, die von Deutschland aus bspw. islamistische und andere extremistische Aktivitäten im Ausland unterstützen und so auswärtige Interessen Deutschlands gefährden. Somit werden die Verfassungsschutzbehörden zur Inlandsaufklärung tätig.

Die Ämter für Verfassungsschutz sind ein wichtiger Bestandteil der Exekutive in unserem freiheitlich demokratischen Rechtsstaat, ebenso wie die Polizei, die insbesondere nach Maßgabe des Polizeirechts für Gefahrenabwehr und im Rahmen der Strafprozessordnung für Straftatenverfolgung zuständig ist. Eine im Vergleich zur übrigen Verwaltung privilegierte Sonderstellung haben diese Behörden mit Blick auf die Informationsfreiheit und die damit verbundene Transparenz einer demokratisch fundierten Verwaltungsorganisation nach Maßgabe unserer Verfassung aber nicht.

Angemessene Begrenzung des Informationszugangs

Sachgerecht wäre eine Regelung im hessischen Informationsfreiheitsrecht, die Informationen für die Fallkonstellationen ausschließt, in denen die Bekanntgabe nachteilige Auswirkungen auf die Aufgabenwahrnehmung des Landesamtes für Verfassungsschutz bzw. der Polizei hätte.

Eine solche Regelung würde sich in das Hessische Informationsfreiheitsrecht auch konsistent einfügen. Denn so ist insbesondere schon jetzt geltendes Recht, dass Informationszugang dann nicht besteht, wenn die Bekanntgabe von Informationen nachteilige Auswirkungen auf Belange der äußeren oder öffentlichen Sicherheit hätte, § 82 Nr. 2 b) HDSIG. Die Korrelation mit der Aufgabenstellung von Verfassungsschutz und Polizei ist hier evident.

§ 82 HDSIG
Ein Anspruch auf Informationszugang besteht nicht…
(…)
2. bei Informationen, deren Bekanntgabe nachteilige Auswirkungen haben kann auf
(…)
b) Belange der äußeren oder öffentlichen Sicherheit
(…)

Zusätzlich kommt alternativ noch eine weitere gesetzgeberische Option hinzu, den absoluten Informationszugangsausschluss abzumildern zugunsten einer differenzierenden und damit auch in der Sache ausgewogenen Regelung:

In Anlehnung an die in § 81 Abs. 1 HDSIG zu erkennende Regelungskonzeption, die Kernfunktionen der dort genannten Stellen vom Informationszugang auszunehmen, könnte ebenso der Informationszugang zu den Kernfunktionen von Polizei und Verfassungsschutz exkludiert, aber für den allgemeinen Verwaltungsbereich dieser Stellen eröffnet werden. Beispielsweise könnten

dann Informationen etwa zur Gebäudemiete oder zu den Fuhrparkkosten mit Erfolg beantragt werden.

Der Hessische Landtag/die Hessische Landesregierung sollten also im Sinne eines konzisen hessischen Informationsfreiheitsrechts den Informationszugang auch gegenüber dem Landesamt für Verfassungsschutz und den Polizeibehörden zugunsten einer differenzierenden Regelung statt eines absoluten Informationszugangsausschlusses informationsfreiheitsfreundlicher ausgestalten.

3. Informationszugang betreffend die Versicherungsaufsicht

Ein Anspruch auf Informationszugang gegenüber dem Hessischen Ministerium für Soziales und Integration in seiner Funktion als Aufsichtsbehörde für die Unfallkasse Hessen besteht nicht, wenn das Bekanntwerden der Informationen nachteilige Auswirkungen auf diese Aufsichtsaufgabe des Ministeriums haben kann.

Das Hessische Ministerium für Soziales und Integration berichtete mir über den Informationsfreiheitsantrag eines Bürgers, den dieser bei dem Ministerium eingereicht hatte und der den Aufgabenbereich des Ministeriums als Aufsichtsbehörde über die Unfallkasse Hessen betraf. Es stelle sich die Frage, ob das Ministerium in diesem Fall als Versicherungsaufsichtsbehörde mit Blick auf das Hessische Informationsfreiheitsrecht anzusehen ist, § 82 Nr. 2 c) HDSIG.

Rechtliche Bewertung

Die Thematisierung des Ministeriums, ob es hinsichtlich der Unfallkasse Hessen als Versicherungsaufsichtsbehörde einzustufen ist, hatte ihren Grund in der Festlegung des Hessischen Informationsfreiheitsrechts, dass in einem solchen Fall kein Anspruch auf Informationszugang besteht, wenn das Bekanntwerden nachteilige Auswirkungen auf die Aufsichtsaufgaben haben kann, § 82 Nr. 2. c) HDSIG.

§ 82 HDSIG
Ein Anspruch auf Informationszugang besteht nicht
(…)
2. bei Informationen, deren Bekanntgabe nachteilige Auswirkungen haben kann auf
(…)
c) die Kontroll-, Vollzugs- oder Aufsichtsaufgaben der Finanz-, Regulierungs-, Sparkassen, Versicherungs- und Wettbewerbsaufsichtsbehörden
(…)

Der Begriff Versicherungsaufsichtsbehörde ist im HDSIG nicht näher definiert, und auch in der Begründung des Gesetzentwurfs gibt es zu diesem Begriff keine weiteren Hinweise (vgl. Landtags-Drucks. 19/5728 S. 151 zu § 82).

Immerhin wird aber in der Begründung die Sparkassenaufsicht explizit genannt (a. a. O.), womit unter Berücksichtigung des Regelungstextes von § 82 Nr. 2 c)

HDSIG endgültig klar ist, dass im amtlichen Gesetzestext hinter „Sparkassen“ das Trennungszeichen offenkundig vergessen wurde. Schon wegen der (richtigerweise gemeinten) Nennung der Sparkassenaufsicht in der Regelung liegt es mit Blick auf Sparkassen als Anstalten des öffentlichen Rechts nahe, dass dementsprechend mit Versicherungen in diesem Aufsichtskontext Versicherungen der öffentlichen Hand, also eben hessische Körperschaften des öffentlichen Rechts gemeint sind. Ein Beispiel wäre hier also auch die Unfallkasse Hessen als gesetzlicher Unfallversicherungsträger im Sinne des Sozialgesetzbuchs VII. Folglich ist dann auch das Hessische Ministerium für Soziales und Integration mit dem Begriff Versicherungsaufsichtsbehörde in § 82 Nr. 2 c) HDSIG im vorliegenden Kontext gemeint.

Zwar könnte man vom Wortlaut her hinsichtlich des Terminus „Versicherungsaufsicht“ auch die private Versicherungswirtschaft in Erwägung ziehen, aber gerade diese Versicherungsaufsicht ist ja nicht den Landesbehörden zugewiesen, wie es beispielsweise bei der Datenschutzaufsicht nach Maßgabe der Europäischen Datenschutzgrundverordnung in Verbindung mit dem Bundesdatenschutzgesetz der Fall ist. Vielmehr wird diese Versicherungsaufsicht von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) auf der Grundlage des Versicherungsaufsichtsgesetzes (VAG) wahrgenommen. Das zeigt also, dass das Thema Versicherungsaufsicht im privaten Sektor ohnehin eine Bundesangelegenheit und keine Ländersache ist.

Vor diesem Gesamthintergrund ergibt es dann also allein Sinn, unter Versicherungsaufsicht im Hessischen Informationsfreiheitsrecht die hessische Landesaufsicht über den hessischen öffentlichen Versicherungssektor zu verstehen. Deshalb habe ich das Ministerium für Soziales und Integration auch in seiner Auffassung bestätigt, dass es in seiner Funktion als Aufsichtsbehörde über die Unfallkasse Hessen eine Versicherungsaufsichtsbehörde im Sinne des Hessischen Informationsfreiheitsrechts ist.

4. Kommunale Informationsfreiheitssatzungen ohne Anwendung des HDSIG

Soweit Kommunen sich dafür entscheiden, kommunale Informationsfreiheitssatzungen einzuführen, ohne das hessische Informationsfreiheitsgesetz als Bezug zu nehmen, ist der Hessische Informationsfreiheitsbeauftragte nicht in seiner gesetzlichen Zuständigkeit betroffen.

Anfangs des Jahres 2020 trug mir die Bürgerrechtsgruppe „*die*Datenschützer Rhein Main" vor, dass sie gestützt auf einen Vorschlag des Bündnisses „Informationsfreiheit für Bayern" einen Musterentwurf für eine kommunale Informationsfreiheitssatzung ausgearbeitet habe, mit dem sie sich an Kommunen in Hessen, insbesondere in der Region Rhein-Main, wenden wolle, um die Informationsfreiheit auf kommunaler Ebene voranzubringen.

Die Bürgerrechtsgruppe bat mich in diesem Zusammenhang, zu ihrem Musterentwurf Stellung zu nehmen. Diese mir vorgelegte „Mustersatzung Informationsfreiheit für Städte und Gemeinden in Hessen" ist als „Transparenz- und Informationsfreiheitssatzung Stadt / Gemeinde" vorgesehen und enthält elf einzelne Paragraphen. Es handelt sich also um ein Satzungskonzept, das außerhalb der Regelungen des Hessischen Datenschutz- und Informationsfreiheitsgesetzes liegt.

Rechtsposition des Hessischen Informationsfreiheitsbeauftragten

Ich habe der Bürgerrechtsgruppe mitgeteilt, dass ich mich mit ihrem Satzungsentwurf nicht befassen werde. Das hat folgenden Hintergrund, den ich der Bürgerrechtsgruppe erläutert habe.

Der Hessische Gesetzgeber regelt in § 81 Abs. 1 Nr. 7 HDSIG, dass die Vorschriften über den Informationszugang auch für die Kommunen gelten, soweit die Anwendung der informationsfreiheitsrechtlichen Vorschriften des Gesetzes (Vierter Teil, §§ 80 ff. HDSIG) durch Satzung ausdrücklich bestimmt wird.

§ 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.

Von dieser kommunalen Hauptregelung abgesehen, gibt es im HDSIG noch eine ergänzende Vorschrift in § 88 Abs. 2 HDSIG, die festlegt, dass in diesem Fall, also der ausdrücklichen Anwendungsbestimmung durch Satzung, auch die Kosten nach Maßgabe der Satzung erhoben werden. In § 88 Abs. 2 HDSIG wird im amtlichen Gesetzestext infolge eines Redaktionsversehens nicht, wie es korrekt wäre, auf § 81 Abs. 1 Nr. 7 HDSIG verwiesen, sondern fehlerhaft auf „§ 81 Satz 1 Nr. 6“. Dieser Fehler resultiert daher, dass im Gesetzentwurf (LT-Drucks. 19/5728) der kommunale Satzungsvorbehalt betreffend die Geltung des hessischen Informationsfreiheitsrechts ursprünglich in § 81 Abs. 1 Nr. 6 vorgesehen war und bei der späteren Veränderung im Gesetzgebungsverfahren zu Nr. 7 die Kostenvorschrift in § 88 Abs. 2 HDSIG nicht korrigierend von Nr. 6 zu Nr. 7 aktualisiert worden ist.

Für den Weg, durch ausdrückliche Satzungsbestimmung das hessische Informationsfreiheitsrecht auf kommunaler Ebene einzuführen, haben sich mittlerweile einige Kommunen entschieden (z. B. die Landkreise Marburg-Biedenkopf, Darmstadt-Dieburg, Groß-Gerau sowie die Städte Kassel und Neu-Isenburg), wenn auch die große Mehrheit der Kommunen es offenbar vorzieht, Bürgeranfragen ohne Bindung an die gesetzlichen Vorgaben im Sinne der §§ 80 ff. HDSIG zu bearbeiten.

Die Zuständigkeit des Hessischen Informationsfreiheitsbeauftragten ist in einer speziellen Norm näher geregelt, nämlich § 89 HDSIG, und diese Regelung bestimmt die Zuständigkeit implizit nur für solche Kommunen, die im Sinne von § 81 Abs. 1 Nr. 7 das Hessische Informationsfreiheitsrecht, also den Vierten Teil des HDSIG, in den kommunalen Rechtsbereich integriert haben.

§ 89 HDSIG

(1) Jeder, der sich in seinem Recht nach dem Vierten Teil verletzt sieht, kann unbeschadet anderweitiger Rechtsbehelfe die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten anrufen.

(…)

(3) (…)

Stellt die oder der Hessische Informationsfreiheitsbeauftragte Verstöße gegen die Vorschriften des Vierten Teils fest, kann sie oder er ihre Behebung in angemessener Frist fordern.

(…)

Mit Blick auf diese gesetzlichen Vorgaben habe ich dem Anliegen der Bürgerrechtsgruppe, außerhalb des Vierten Teils des HDSIG einen selbst gefertigten kommunalen Satzungsentwurf zu würdigen, nicht entsprochen.

5. Informationszugang hinsichtlich der WLAN-Struktur öffentlicher Stellen

Der Informationszugang betreffend die WLAN-Struktur öffentlicher Stellen wird vom Hessischen Beauftragten für Informationsfreiheit unterstützt. In dieser Angelegenheit kam es zur Zusammenarbeit mit der Bundesnetzagentur.

Ein Bürger beschwerte sich bei mir darüber, dass er an die Hochschulen des Landes Hessen betreffend deren WLAN-Struktur Informationsfreiheitsanträge gerichtet habe, diese aber entweder überhaupt nicht beantwortet oder aber unter Hinweis auf Sicherheitsbedenken abschlägig beschieden worden seien.

Der Informationszugangsantrag hatte folgende Fassung:

„Sind die WLAN Systeme (z. B. die Eduroam zur Verfügung stellen) der Hochschule so eingestellt, dass diese z. B. durch eine Rogue Accesspoint Containment Funktion andere WLAN Signale mithilfe von Deauth/Deassociationspaketen stören?

Wenn ja warum und welche Einstellungen liegen vor?

Wenn nein warum?“

Zusammenarbeit mit der Bundesnetzagentur

Der Inhalt dieses Informationszugangsantrages war für mich Anlass, in der Sache Kontakt zur Bundesnetzagentur aufzunehmen und mit dieser die Angelegenheit zu erörtern. Der Informationsfreiheitsantrag betrifft das Thema, ob eine bestimmte Technik, die im Rahmen der Allgemeinzuteilungen der WLAN-Frequenzen gemäß § 55 Abs. 2 Telekommunikationsgesetz (TKG) durch die Bundesnetzagentur ausdrücklich als unzulässig bewertet wird, zum Einsatz kommt.

Da nur eine detaillierte Beauskunftung des Informationsfreiheitsantrags sicherheitsrelevante Aspekte berühren könnte, habe ich den betroffenen Hochschulen vorgeschlagen, dem Beschwerdeführer (soweit zutreffend) mitzuteilen, dass die Nutzung der WLAN-Netze ausschließlich im Rahmen der Vorgaben der aktuell veröffentlichten Allgemeinzuteilungen erfolgt. Demzufolge könnte die Antwort wie folgt aussehen:

„Aussendungen, die absichtliche bestimmte WLAN-Nutzungen stören oder verhindern, wie z. B. Aussendungen von Funksignalen und/oder Datenpaketen, die die Abmeldung oder Beeinflussung von WLAN-Verbindungen anderer

Nutzer gegen deren Willen zum Ziel haben, sind nicht gestattet und werden an der Hochschule nicht eingesetzt.“

Der Beschwerdeführer meldete sich nach geraumer Zeit wieder und teilte mit, seine Beschwerden seien erledigt, seine Informationsfreiheitsanträge seien nunmehr beauskunftet worden.

6. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr ergab sich ein geringer Anstieg an Beschwerden und Beratungen.

IFG	2019	2020
Beschwerden	61	64
Beratungen	42	47

ANHANG zu II

Im Jahr 2020 wurden von der Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder (IFK) keine Entschließungen, Beschlüsse oder Materialien gefasst.

Sachwortverzeichnis